

Geavanceerde onbewerkte versie

Distr.: Algemeen
11 oktober 2019

Oorspronkelijk: Engels

Vierenzeventigste zitting

Punt 72(b) van de voorlopige agenda*

Bevordering en bescherming van mensenrechten:

Mensenrechtenkwesities, inclusief alternatieve benaderingen

voor het verbeteren van de daadwerkelijke uitoefening van mensenrechten
en fundamentele vrijheden

Verslag van de speciale rapporteur voor extreme armoede en mensenrechten**

Nota van de secretaris-generaal

De Secretaris-Generaal heeft de eer om aan de Algemene Vergadering het rapport van de Speciale Rapporteur voor extreme armoede en mensenrechten, Philip Alston, voor te leggen overeenkomstig resolutie 35/19 van de Mensenrechtenraad.

Samenvatting

De digitale verzorgingsstaat is al een realiteit of is in veel landen over de hele wereld in opkomst. In deze staten worden systemen voor sociale bescherming en bijstand steeds meer aangedreven door digitale gegevens en technologieën die worden gebruikt om te automatiseren, voorspellen, identificeren, bewaken, opsporen, richten en straffen. Dit rapport erkent de onweerstaanbare aantrekkingskracht voor regeringen om in deze richting te gaan, maar waarschuwt dat er een groot risico bestaat om als zombies in een digitale welvaartsdystopie te belanden. Het betoogt dat Big Tech opereert in een bijna mensenrechtenvrije zone, en dat dit vooral problematisch is wanneer de particuliere sector een leidende rol speelt bij het ontwerpen, bouwen en zelfs exploiteren van belangrijke delen van de digitale verzorgingsstaat. Het rapport beveelt aan dat in plaats van geobsedeerd te zijn door fraude, kostenbesparingen, sancties en marktgestuurde definities van efficiëntie, het uitgangspunt moet zijn hoe socialezekerheidsbudgetten door middel van technologie kunnen worden getransformeerd om een hogere levensstandaard voor de kwetsbaren en kansarmen te waarborgen.

* A/74/50.

** Dit rapport is na de deadline ingediend om de meest recente ontwikkelingen weer te geven.

Inhoud

	<i>Bladzijde</i>
I. Invoering.....	3
II. Gebruik van digitale technologieën in de verzorgingsstaat	5
A. Identiteitsverificatie	5
B. Geschiktheidsbeoordeling	7
C. Berekening en betaling van bijstandsuitkeringen	8
D. Fraudepreventie en -opsporing	8
E. Risicoscore en behoefteclassificatie	9
F. Communicatie tussen welzijnsinstanties en uitkeringsgerechtigden	9
III. Digitale technologieën laten werken voor sociale bescherming.....	10
A. Mensenrechten serieus nemen en dienovereenkomstig reguleren.....	11
B. Zorgen voor wettigheid en transparantie	12
C. Bevordering van digitale gelijkheid.....	13
D. Bescherming van economische en sociale rechten in de digitale verzorgingsstaat	14
E. Bescherming van burgerrechten en politieke rechten in de digitale verzorgingsstaat.....	15
F. Weerstaan aan de onvermijdelijkheid van een toekomst die alleen digitaal is.....	17
G. De rol van de particuliere sector	18
H. Verantwoordingsmechanismen	18
IV. Conclusies	19

I. Inleiding¹

1. Het tijdperk van digitaal bestuur staat voor de deur. In hoge- en middeninkomenslanden, elektronisch stemmen, technologiegestuurde bewaking en controle, onder meer door middel van gezichtsherkenningsprogramma's, op algoritmen gebaseerd voorspellend politiewerk, de digitalisering van justitie- en immigratiesystemen, online indiening van belastingaangiften en betalingen, en vele andere vormen van elektronische interacties tussen burgers en verschillende bestuursniveaus worden de norm. En in lagere inkomenslanden leggen nationale systemen van biometrische identificatie de basis voor vergelijkbare ontwikkelingen, met name in systemen voor sociale bescherming, of 'welzijn', om een afgekorte term te gebruiken.²

Verbeterde sociale voorzieningen, samen met verbeterde veiligheid, is onveranderlijk een van de 2. belangrijkste doelen die worden aangevoerd om de diepgaande maatschappelijke transformaties en enorme uitgaven te rechtvaardigen die gepaard gaan met het verplaatsen van de hele bevolking van een land, niet alleen naar een nationale unieke biometrische identiteitskaart systeem, maar op gekoppelde gecentraliseerde systemen die een breed scala aan overheidsdiensten en de levering van goederen bieden, variërend van voedsel en onderwijs tot gezondheidszorg en speciale diensten voor ouderen of mensen met een handicap.

3. Het resultaat is de opkomst van de 'digitale verzorgingsstaat' in veel landen over de hele wereld.³ In deze staten worden systemen van sociale bescherming en bijstand steeds meer aangedreven door digitale gegevens en technologieën die worden gebruikt om te automatiseren, voorspellen, identificeren, surveilleren, detecteren, richten en straffen. Het proces wordt gewoonlijk 'digitale transformatie' genoemd, maar deze ietwat neutrale term mag het revolutionaire, politiek gedreven karakter van veel van dergelijke innovaties niet verhullen. Commentatoren hebben "een toekomst voorspeld waarin overheidsinstanties effectief wetten kunnen maken door middel van een robot",

⁴ en het is duidelijk dat er nieuwe vormen van governance

ontstaan die sterk afhankelijk zijn van de verwerking van enorme hoeveelheden digitale gegevens uit alle beschikbare bronnen, voorspellende analyses gebruiken om risico's te voorzien, besluitvorming automatiseren en menselijke besluitvormers discretie ontnemen. In zo'n wereld worden burgers steeds zichtbaarder voor hun overheid, maar niet andersom.⁵

Welzijn is een aantrekkelijk instappunt, niet alleen omdat het een groot deel van de 4. nationale begroting opslokt of zo'n groot deel van de bevolking treft, maar ook omdat digitalisering kan worden gepresenteerd als een in wezen goedaardig initiatief. Zo verkondigt de digitale strategie van het Verenigd Koninkrijk bijvoorbeeld dat het "de relatie tussen burgers en de staat zal transformeren", waardoor "meer macht in de handen van burgers wordt gelegd en beter wordt ingespeeld op hun behoeften". In India omvatten de kernwaarden van de Unique Identification Authority of India: het faciliteren van goed bestuur, integriteit, inclusieve natievorming, een gezamenlijke aanpak, excellentie in dienstverlening, en transparantie en openheid.

Met andere woorden, de omarming van de digitale verzorgingsstaat wordt gepresenteerd als een altruïstische en 5. nobele onderneming die is ontworpen om ervoor te zorgen dat burgers profiteren van nieuwe technologieën, een efficiëntere overheid ervaren en een hoger niveau van welzijn genieten. Vaak ging de digitalisering van socialezekerheidsstelsels echter gepaard met forse bezuinigingen op het totale welzijnsbudget, een vernauwing van de begunstigdenpool, de afschaffing van sommige diensten, de introductie van veeleisende en opdringerige vormen van conditionaliteit, het nastreven van gedragsveranderingsdoelen, het opleggen van strengere sanctieregimes en een volledige omkering van het traditionele idee dat de staat verantwoording moet afleggen aan het individu.

¹ Dit rapport is tot stand gekomen in nauwe samenwerking met Christiaan van Veen, directeur van het Digital Welfare States and Human Rights Project, aan de New York University School of Law.

² Hoewel welzijn vaak als een pejoratieve term wordt gebruikt, wordt het in dit rapport in positieve zin gebruikt en is het synoniem met het doel van sociale bescherming, zoals weerspiegeld in het ILO-initiatief Social Protection Floor en vergelijkbare benaderingen. Zie in het algemeen David Garland, *The Welfare State: A Very Short Introduction* (2016).

³ Philip Alston en Christiaan van Veen, 'Hoe de verzorgingsstaat van Groot-Brittannië is overgenomen door schimmige technische adviseurs', *The Guardian*, 27 juni 2019.

⁴ Cary Coglianese en David Lehr, 'Reguleren door robots: administratieve besluitvorming in het tijdperk van machinaal leren', *Georgetown Law Journal* (deel 105, 2017), p. 1147.

⁵ Vergelijk Foucaults beschrijving van panoptische systemen waarin degenen die onder toezicht staan 'gezien worden, zonder ooit te zien'. Michel Foucault, *Discipline en straf: de geboorte van de gevangenis* (1977), p. 202.

6. Deze andere resultaten worden gepromoot in de naam van efficiëntie, doelgerichtheid, het stimuleren van werk, het uitroeien van fraude, het versterken van verantwoordelijkheid, het aanmoedigen van individuele autonomie en het reageren op de vereisten van begrotingsconsolidatie. Door gebruik te maken van vaak ideologisch geladen termen, wordt neoliberal economisch beleid naadloos vermengd met wat wordt gepresenteerd als baanbrekende hervormingen van de sociale zekerheid, die op hun beurt vaak worden gefaciliteerd, gerechtvaardigd en beschermd door nieuwe digitale technologieën. Hoewel deze laatste als 'wetenschappelijk' en neutraal worden gepresenteerd, kunnen ze waarden en veronderstellingen weerspiegelen die ver verwijderd zijn van, en mogelijk in tegenspraak zijn met, de beginselen van de mensenrechten. Bovendien worden, vanwege de relatieve achterstelling en machteloosheid van veel uitkeringsgerechtigden, voorwaarden, eisen en vormen van opdringerigheid opgelegd die nooit zouden zijn geaccepteerd als ze in plaats daarvan waren uitgeprobeerd in programma's die van toepassing zijn op welvarende leden van de gemeenschap.

7. Ondanks de enorme belangen die niet alleen voor miljoenen individuen maar voor de samenleving als geheel op het spel staan, hebben deze kwesties, op een paar opmerkelijke uitzonderingen na, opmerkelijk weinig aandacht gekregen. De reguliere technische gemeenschap heeft zich laten leiden door officiële zorgen over efficiëntie, budgetbesparingen en fraudedetectie. De welvaartsgemeenschap heeft de neiging om de technologische dimensies los te zien van de beleidsontwikkelingen, in plaats van integraal met elkaar verbonden te zijn. En degenen in de mensenrechtengemeenschap die zich met technologie bezighouden, zijn begrijpelijkerwijs in plaats daarvan gefocust op zorgen als de opkomst van de surveillancestaat, de mogelijk fatale ondermijning van de privacy, de zeer discriminerende impact van veel algoritmen en de gevolgen van het opkomende regime van surveillance. kapitalisme.

8. Maar de dreiging van een digitale dystopie is vooral groot in relatie tot de opkomende digitale verzorgingsstaat. Dit rapport heeft tot doel de veronachtzaming van deze kwesties tot nu toe recht te zetten door een systematisch verslag te geven van de manieren waarop digitale technologieën worden gebruikt in de verzorgingsstaat en van de implicaties ervan voor de mensenrechten. Het concludeert met een oproep tot regulering van digitale technologieën, met inbegrip van kunstmatige intelligentie, om de naleving van de mensenrechten te waarborgen, en tot een heroverweging van de positieve manieren waarop de digitale verzorgingsstaat een kracht kan zijn voor het bereiken van sterk verbeterde systemen van sociale bescherming. .

9. Het rapport bouwt gedeeltelijk voort op landenrapporten van de speciale rapporteur over bezoeken aan de Verenigde Staten in 2017 en het Verenigd Koninkrijk in 2018, waarin de aandacht werd gevestigd op het toenemende gebruik van digitale technologieën in socialebeschermingsstelsels. Bij het opstellen van het rapport heeft de speciale rapporteur overleg gepleegd met vertegenwoordigers van verschillende digitale rechtengroepen, vooraanstaande wetenschappers en andere belanghebbenden, eerst tijdens een bijeenkomst georganiseerd door het Digital Freedom Fund in Berlijn in februari 2019, en vervolgens tijdens een andere bijeenkomst gesponsord door het Centrum voor Informatie Technologiebeleid aan de Princeton University in april 2019. 7 Daarnaast resulteerde een formele oproep tot het indienen van bijdragen in zo'n 60 inzendingen uit 34 landen, waaronder 22 regeringen, evenals internationale en nationale maatschappelijke organisaties, nationale mensenrechteninstellingen, academici en individuen. Hoewel het onmogelijk is om recht te doen aan deze rijke en gedetailleerde bijdragen in zo'n noodzakelijkerwijs beknopt rapport, heeft de Speciale Rapporteur ze elektronisch beschikbaar gesteld⁹ en zal ze blijven analyseren in het kader van het lopende werk aan de digitale verzorgingsstaat.¹⁰

⁶ Zie Virginia Eubanks, *Automating Inequality* (2018) voor baanbrekend werk over de impact van digitale technologieën op de Amerikaanse verzorgingsstaat, met name op de armste individuen in het systeem. Zie ook Cathy O'Neil, *Weapons of Math Destruction* (2016) en Khiara Bridges, *The Poverty of Privacy Rights* (2017).

⁷ <https://www.princeton.edu/news/2019/04/18/panelists-tell-un-expert-artificial-intelligence-offers-promise-and-peril-social>.

⁸ Uit: Argentinië, Australië, Oostenrijk, Azerbeidzjan, Brazilië, Chili, Kroatië, Egypte, El Salvador, Estland, Duitsland, Griekenland, Guatemala, India, Italië, Ierland, Kazachstan, Libanon, Mexico, Nicaragua, Nigeria, Nederland, Nieuw-Zeeland, Oman, Pakistan, Filipijnen, Polen, Qatar, Russische Federatie, Senegal, Zuid-Afrika, Zwitserland, het Verenigd Koninkrijk en de Verenigde Staten.

⁹ <https://www.ohchr.org/EN/Issues/Poverty/Pages/SubmissionsGADigitalTechnology.aspx>.

¹⁰ <https://chrgj.org/people/christiaan-van-veen/>.

II. Gebruik van digitale technologieën in de verzorgingsstaat

10. Uit de vele ontvangen inzendingen en op basis van verschillende casestudy's die in de literatuur aan de orde komen, is het mogelijk om verschillende manieren en verschillende stadia in de welzijnscontext te onderscheiden waarin digitale innovatie het meest prominent is gebruikt.

A. Identiteitsverificatie

11. Het vaststellen van ieders juridische identiteit, onder meer door geboorteregistratie, tegen het jaar 2030 is het doel van Sustainable Development Goal (SDG) 16.9. Een verifieerbare identiteit is essentieel voor het aanvragen van uitkeringen, het vaststellen van rechten, het ontvangen van uitkeringen en het aantekenen van bezwaar tegen weigering. Voor de overheid of een andere aanbieder voorkomt het dubbel werk en fraude, vergemakkelijkt het nauwkeurige targeting en verhoogt het de efficiëntie. Van oudsher worden papieren en/of plastic documenten gebruikt in vormen als geboorteakten, identiteitskaarten en paspoorten. Deze systemen functioneren redelijk goed in het grootste deel van het Globale Noorden, hoewel 21 miljoen volwassenen in de Verenigde Staten geen door de overheid uitgegeven identiteitsbewijs met foto hebben. 11 In het Globale Zuiden hebben 502 miljoen mensen in Afrika bezuiden de Sahara en 357 miljoen in Zuid-Azië geen officiële identificatie.¹² In Liberia bijvoorbeeld bedraagt de geboorteregistratie slechts 5 procent en werden de nationale identiteitskaarten pas in 2015 ingevoerd.¹³

12. Als reactie daarop hebben de Wereldbank, regionale ontwikkelingsorganisaties en bilaterale donoren nieuwe programma's gelanceerd om de toegang tot identiteitsdocumenten te bevorderen. Met name de 'ID4D'-campagne (Identification for Development)¹⁴ van de Wereldbank is sterk gericht op het promoten van digitale technologieën als de belangrijkste oplossing. Dit staat expliciet in de 'Principles on Identification for Sustainable Development', die breed worden onderschreven, ook door MasterCard. 15

13. De Principles erkennen dat er zowel voor- als nadelen aan verbonden zijn. Aan de positieve kant wordt beweerd dat digitale technologie "enorme besparingen kan opleveren voor burgers, overheden en bedrijven door de transactiekosten te verlagen, de efficiëntie te verhogen en innovatie in de dienstverlening te stimuleren, met name voor de armste en meest kansarme groepen in de samenleving". 16 Digitale identiteitssystemen kunnen ook "het bestuur verbeteren, financiële inclusie stimuleren, genderongelijkheid verminderen door vrouwen en meisjes mondiger te maken, en de toegang tot gezondheidsdiensten en sociale vangnetten voor de armen verbeteren".¹⁷

14. Maar naast dit indrukwekkende en inmiddels bekende verkooppraatje, erkennen de Principles en vergelijkbare documenten¹⁸ ook mogelijke nadelen, variërend van politieke terugslag tot zorgen over privacy en (cyber)veiligheid. Oplossingen voor het omgaan met die risico's zijn vaak technologisch of nemen de vorm aan van soft law-normen. Zo roept een vergelijkbaar document van de United States Agency for International Development (USAID) op tot "open source-oplossingen" en het ontwikkelen van goede "praktijken voor gegevensprivacy" om de relevante problemen op te lossen. Terwijl de Wereldbank-beginselen verwijzen naar geïsoleerde mensenrechtenbeginselen, zoals artikel 7 van de

¹¹ <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/PrivacyInternational.pdf>

¹² USAID, 'Identiteit in een digitaal tijdperk' (2017), p. 8.

¹³ Bronwen Manby, *Burgerschap in Afrika* (2018), p. 3.

¹⁴ <https://id4d.worldbank.org/>

¹⁵ Wereldbank en Centrum voor Wereldwijde Ontwikkeling, 'Principles on Identification for Sustainable Development: Toward the Digital Age', februari 2017, op <http://documents.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-voor-duurzame-ontwikkeling-naar-het-digitale-tijdperk.pdf>

¹⁶ Wereldbank en Centrum voor Wereldwijde Ontwikkeling, 'Principles on Identification for Sustainable Ontwikkeling: op weg naar het digitale tijdperk', februari 2017, p. 5, beschikbaar op: <http://documents.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf>; 17 idd.

¹⁸ USAID, 'Identiteit in een digitaal tijdperk' (2017); McKinsey, 'Digital Identification: A Key to Inclusive Growth', januari 2019, op <https://www.mckinsey.com/~media/mckinsey/featured%20insights/innovation/the%20value%20of%20digital%20id%20for%20the%20global%20economy%20and%20society/digital-id-a-key-to-inclusive-growth-january%202019.ashx>

Verdrag inzake de Rechten van het Kind, baseren ze zich in de eerste plaats op de noodzaak om een interoperabel systeem te creëren dat gebruikmaakt van open standaarden en 'privacy door systeemontwerp' beschermt.

15. Het grootste biometrische identificatiesysteem ter wereld is Aadhaar in India, een 12-cijferig uniek identificatienummer uitgegeven aan inwoners van India. Het bevat zowel demografische als biometrische informatie, waaronder een irisscan, een foto en vingerafdrukken. Het wordt gebruikt om de identiteit van ontvangers van uitkeringen en subsidies te verifiëren en is nu verplicht om toegang te krijgen tot die sociale rechten.¹⁹ Het werd voor het eerst geïntroduceerd in 2009 en omvat nu meer dan 1,2 miljard mensen²⁰ en wordt enthousiast onderschreven door de internationale ontwikkelingsgemeenschap.²¹ De Wereldbank prees het voor het "overwinnen van complexe informatieproblemen, [daardoor] bereidwillige regeringen helpend om de inclusie van kansarme groepen te bevorderen",

22 en andere regeringen enthousiast heeft aangemoedigd om van de ervaring te leren,²³ en naar verluidt hebben meer dan 20 landen belangstelling getoond om Aadhaar na te volgen.²⁴

16. Toch blijft het controversieel in eigen land. Critici zijn naar verluidt lastiggevalen en in de gaten gehouden vanwege hun tegenstand,²⁵ en de regeling is bekritiseerd vanwege het onnodig verzamelen van biometrische informatie, vanwege ernstige tekortkomingen in wetgevend toezicht, functiekruip, het faciliteren van toezicht en andere inbreuken op het recht op privacy, het verergeren van cyberbeveiligingsproblemen en het creëren van belemmeringen voor toegang tot een reeks sociale rechten.²⁶

17. In 2018 bevestigde het Indiase Hooggerechtshof in een historische uitspraak van 1448 pagina's de grondwettigheid van Aadhaar, zij het met enkele voorbehouden. De rechtbank leek het gebruik van biometrische identificatietechnologie in het kader van het verstrekken van sociale voorzieningen als legitiem, proportioneel en zelfs onvermijdelijk te beschouwen. In een verzorgingsstaat was het doel van Aadhaar om ervoor te zorgen dat uitkeringen de beoogde begunstigde bereiken "natuurlijk een legitiem doel van de staat".²⁷ rechten,²⁸ en ging zelfs zo ver om Aadhaar te typeren als "een vitaal instrument om goed bestuur in een sociale verzorgingsstaat te waarborgen".²⁹ Maar de uitspraak van het Hooggerechtshof heeft blijkbaar geen einde gemaakt aan de controverse rond het plan.³⁰

18. In 2019 eiste Kenia van al zijn burgers, ook degenen die in het buitenland wonen, en alle buitenlanders en vluchtelingen in het land, ouder dan 6 jaar, een nationaal identiteitsbewijs te verkrijgen om toegang te krijgen tot overheidsdiensten, waaronder sociale uitkeringen.³¹ Dit omvatte het verstrekken van biometrische gegevens, waaronder vingerafdrukken, handgeometrie, oorlelgeometrie, retina- en irispatronen, stemgolven en DNA in digitale vorm. In reactie op een zaak waarin wordt beweerd dat deze Huduma Namba programma de rechten op privacy, gelijkheid, non-discriminatie en inspraak schond, vaardigde het Hooggerechtshof een voorlopig bevel uit waardoor het registratieproces kon worden voortgezet, maar op vrijwillige basis en op basis van het feit dat de uitbetaling van overheidsdiensten en -uitkeringen niet kon worden voorwaardelijk gemaakt voor deelname. Vervolgens is de inschrijving verlopen

¹⁹ Zie bijvoorbeeld Centre for Communication Governance aan de National Law University Delhi, op <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/NationalLawUniversityDelhi.pdf>.

²⁰ <https://economictimes.indiatimes.com/news/politics-and-nation/national-population-register-to-include-aadhaar-details/articleshow/70528850.cms?from=mdr>.

²¹ Jeanette Rodrigues, 'India ID Program Wins World Bank Praise Ondanks 'Big Brother' Fears', 15 maart 2017, beschikbaar via: <https://www.bloomberg.com/news/articles/2017-03-15/india-id-program-wint-wereldbank-lofte-midden-van-big-brother-angsten>.

²² Wereldbank, *Wereldontwikkelingsrapport 2016*, p. 2.

²³ <https://www.livemint.com/Politics/UEQ9o8Eo8RiaAaNNMyLbEK/Aadhaar-goes-global-finds-takers-in-Russia-and-Africa.html>.

²⁴ <https://factordaily.com/aadhaar-india-stack-export/>.

²⁵ <https://www.reuters.com/article/us-india-aadhaar-breach/critics-of-indias-id-card-project-say-they-have-been-harassed-put-under-surveillance-idUSKBN1FX0H0>

²⁶ Indiening bij de speciale rapporteur door de National Law University, Delhi.

²⁷ Hooggerechtshof van India, schriftelijke petitie (burgerlijk) nr. 494 van 2012, p. 341.

²⁸ Id., p. 377.

²⁹ Id., p. 553.

³⁰ <https://www.nytimes.com/2018/09/26/technology/india-id-aadhaar-supreme-court.html>.

³¹ Amnesty International, op <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/AmnestyInternational.pdf>.

in rap tempo is ongeveer tweederde van de bevolking geregistreerd, 32 en de regering dreigt naar verluidt niet-geregistreerde personen uit te sluiten van toegang tot uitkeringen of het recht om te stemmen.³³

19. In Zuid-Afrika verstrekt de South African Social Security Agency (SASSA) premievrije en inkomensafhankelijke sociale uitkeringen aan ongeveer een derde van de bevolking, waaronder bijvoorbeeld uitkeringen voor kinderbijslag, voor gepensioneerden en voor personen met een handicap.³⁴ In 2012 sloot SASSA een contract met het bedrijf Cash Paymaster Services (CPS), een dochteronderneming van Net1, om de subsidies te verstrekken.³⁵ CPS geregistreerde begunstigden door hun biometrische informatie te verzamelen (vingerafdrukken en oorspronkelijk stemopnamen) en begunstigden werden uitgegeven MasterCard-betaalpassen met biometrische functionaliteit en een gekoppelde bankrekening door Net1 en Grindrod Bank in samenwerking met SASSA.³⁶ Na veel controverse rond de aanbesteding bij CPS, de door CPS in rekening gebrachte vergoedingen, inhoudingen op sociale subsidies op deze rekeningen en privacykwesties rond de verwerking van kaarthoudergegevens veranderde SASSA in 2018 van provider door een samenwerking aan te gaan met het South African Post Office (SAPO).

SASSA en SAPO zullen nieuwe biometrische kaarten verstrekken. De overgang van CPS naar SAPO was complex en heeft geleid tot vragen over de effectieve toegang tot sociale subsidies door begunstigden in Zuid-Afrika.³⁷

20. Er zijn nog veel meer voorbeelden te geven van landen die digitale identiteitssystemen gebruiken of verkennen, waaronder Argentinië,³⁸ Bangladesh,³⁹ Chili,⁴⁰ Ierland, Jamaica,⁴¹ Maleisië,⁴² de Filipijnen,⁴³ en de Verenigde Staten.⁴⁴

B. Geschiktheidsbeoordeling

21. Geautomatiseerde programma's worden in veel landen steeds vaker gebruikt om te beoordelen of iemand in aanmerking komt. Een bijzonder leerzaam geval was de automatisering van beslissingen over geschiktheid in Ontario in 2014 via het Social Assistance Management System (SAMS), dat steunde op Cúram, een aanpasbaar kant-en-klaar IBM-softwarepakket dat ook wordt gebruikt in welzijnsprogramma's in Canada, de Verenigde Staten, Duitsland, Australië en Nieuw-Zeeland.⁴⁵

22. In 2015 rapporteerde de auditeur-generaal van Ontario over 1.132 gevallen van fouten met vaststellingen van geschiktheid en betalingsbedragen onder SAMS waarmee ongeveer \$ 140 miljoen gemoeid was. De totale uitgaven aan SAMS bedroegen eind 2015 290 miljoen dollar.⁴⁶ Het nieuwe systeem zou er naar verluidt toe hebben geleid dat dossierbehandelaars hun toevlucht namen tot uitvluchten om ervoor te zorgen dat begunstigden eerlijk werden behandeld, dat beslissingen zeer moeilijk te begrijpen waren en dat het personeel veel extra werk met zich meebracht.⁴⁷

³² idd.

³³ <https://www.standardmedia.co.ke/article/2001334286/you-ll-miss-vital-services-without-huduma-namba>.

³⁴ <https://www.dfa.co.za/news/budget2019-social-grants-to-increase-19404725>.

³⁵ Black Sash, op <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/BlackSash.pdf>.

³⁶ <https://newsroom.mastercard.com/press-releases/more-than-2-5-million-mastercard-debit-cards-issue-to-social-welfare-beneficiaries-in-south-africa/>.

³⁷ <https://citizen.co.za/business/1944057/post-office-set-to-take-over-cash-payments-from-cps/>.

³⁸ Indiening bij de speciale rapporteur door de regering van Argentinië.

³⁹ <https://privacyinternational.org/examples/2878/bangladesh-biometrics-needed-access-welfare-betaling>.

⁴⁰ In Chili wordt gezichtsherkenningstechnologie gebruikt om schoolmaaltijden te bezorgen: zie <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/PrivacyInternational.pdf>.

⁴¹ <https://opm.gov.jm/portfolios/national-identification-system/>.

⁴² <https://www.opengovasia.com/malaysias-digital-id-project-to-be-finalised-by-2019/>.

⁴³ <https://psa.gov.ph/philsys>.

⁴⁴ Zie bijvoorbeeld het gebruik van digitale technologieën in het CalWORKs-programma in Californië, de Verenigde Staten,

op <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/HumanRightsWatch.pdf>.

⁴⁵ Indiening bij de speciale rapporteur door Human Rights Watch, verkrijgbaar bij:

<https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/HumanRightsWatch.pdf>.

⁴⁶ *Jaarverslag 2015 van het bureau van de auditeur-generaal van Ontario*, p. 475.

⁴⁷ Jennifer Raso, 'Displacement as Regulation: New Regulatory Technologies and Front Line Decision Making in Ontario Works', *Canadian Journal of Law and Society*, Vol. 32, (2017) 75.

C. Berekening en uitkeringen van bijstandsuitkeringen

23. De berekening en betaling van uitkeringen gebeurt steeds vaker via digitale technologieën zonder tussenkomst van dossierbehandelaars en andere menselijke besluitvormers.

Hoewel dergelijke systemen veel potentiële voordelen bieden, ontving de Speciale Rapporteur ook informatie over prominente voorbeelden van systeemfouten of storingen die voor grote aantallen begunstigden tot grote problemen leidden. Het ging onder meer om het 'Robodebt'-fiasco in Australië⁴⁸, het Real Time Information-systeem in het Verenigd Koninkrijk⁴⁹ en het SAMS-systeem in Canada.

24. Ook aan uitkeringsgerechtigden worden steeds vaker elektronische betaalkaarten of debetkaarten verstrekt. Uit informatie die aan de speciale rapporteur is verstrekt met betrekking tot dergelijke programma's in Nieuw-Zeeland, Australië en Zuid-Afrika, blijkt dat de problemen sterk op elkaar lijken. Ten eerste hebben begunstigden vaak moeite om toegang te krijgen tot hun recht op sociale zekerheid en deze volledig te benutten.⁵⁰ Ten tweede, wanneer dergelijke kaarten duidelijk herkenbaar zijn als welzijnsgerelateerd, hebben gebruikers gevoelens van machteloosheid, gêne en schaamte geuit.⁵¹ een probleem dat nog groter wordt wanneer de gebruikers afkomstig zijn uit gemeenschappen die al lang gewend zijn aan uitsluiting.⁵² Ten derde maken elektronische kaarten het mogelijk om gedragsgegevens te monitoren en te bewaken door welzijnsinstanties en particuliere actoren, waardoor belangrijke mensenrechtenkwesies.⁵³

25. Ten vierde heeft de uitbesteding van de uitgifte en het beheer van elektronische kaarten aan particuliere bedrijven tot problemen geleid, zoals het aanmoedigen van gebruikers om te betalen voor commerciële financiële producten en het opleggen van gebruikersvergoedingen.⁵⁴ Meer in het algemeen weerspiegelt het ethos rond dergelijke kaarten vaak stereotypen zoals de financiële onbetrouwbaarheid en irrationaliteit van mensen die in armoede leven.

D. Fraudepreventie en -opsporing

26. Fraude en fouten in socialezekerheidsstelsels kunnen potentieel zeer grote sommen geld met zich meebrengen en zijn al lange tijd een grote zorg voor regeringen. Het is dan ook niet verwonderlijk dat veel van de ingevoerde digitale socialezekerheidsstelsels zijn ontworpen met een bijzondere nadruk op het vermogen om gegevens uit verschillende bronnen te matchen om bedrog en onregelmatigheden van de kant van bijstandsaanvragers aan het licht te brengen. Desalniettemin suggereert bewijs van landmissies die door de speciale rapporteur zijn ondernomen⁵⁵ samen met andere onderzochte gevallen⁵⁶ dat de omvang van deze problemen vaak wordt overschat en dat er soms een geheel onevenredige aandacht is voor deze specifieke dimensie van de complexe welzijnsvergelijking.

Afbeeldingen van personen die zogenaamd totaal onwaardig zijn en hoge uitkeringen van de overheid ontvangen, zoals Ronald Reagan's 'bijstandskoningin'-trope, worden al lang door conservatieve politici gebruikt om het concept van sociale bescherming zelf in diskrediet te brengen. Het risico is dat de digitale verzorgingsstaat eindeloze mogelijkheden biedt om toezicht en inbraak naar nieuwe en zeer problematische hoogten te tillen.

⁴⁸ Terry Carney, 'De nieuwe digitale toekomst voor welzijn: schulden zonder wettelijk bewijs of morele autoriteit?', *UNSW Law Journal Forum* (maart 2018) p. 1; Rapport van de waarnemend ombudsman van het Gemenebest, Richard Glenn, 'Centrelink's geautomatiseerd systeem voor het innen en innen van schulden', april 2017, p. 7-8; Indiening bij de speciale rapporteur door Monash University.

⁴⁹ Verklaring over bezoek aan het Verenigd Koninkrijk, 16 november 2018, op: <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23881&LangID=E>.

⁵⁰ <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/GriffithUniversity.docx>.

⁵¹ <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/NicoleNaujokas.docx>.

⁵² [https://www.theguardian.com/australia-news/2017/jan/09/ration-days-again-cashless-welfare-card ignites-shame](https://www.theguardian.com/australia-news/2017/jan/09/ration-days-again-cashless-welfare-card-ignites-shame).

⁵³ <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/UniversityAuckland.docx>.

⁵⁴ <http://theconversation.com/the-real-risks-behind-south-africas-social-grant-payment-crisis-73224>

⁵⁵ Verklaring over het bezoek aan het Verenigd Koninkrijk, door professor Philip Alston, speciale VN-rapporteur voor extreme armoede en mensenrechten, 16 november 2018, beschikbaar op: <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23881&LangID=E>.

⁵⁶ Zie de SyRI-casus uit Nederland, n86 hieronder.

E. Risicoscore en behoefteclassificatie

27. Risicoberekening vormt onvermijdelijk de kern van het ontwerp van sociaalezekerheidsstelsels en digitale technologieën kunnen in dit opzicht zeer geavanceerd zijn. Naast het opsporen en voorkomen van fraude is kindbescherming een belangrijk aandachtspunt op dit gebied, zoals blijkt uit voorbeelden uit uiteenlopende landen als de Verenigde Staten,⁵⁷ Nieuw-Zeeland,⁵⁸ het Verenigd Koninkrijk,⁵⁹ en Denemarken.⁶⁰ Overheden hebben deze technieken ook toegepast om te bepalen of werkloosheidssteun zal worden verstrekt en op welk niveau. Een prominent dergelijk systeem in Polen werd als ongrondwettelijk beschouwd,⁶¹ maar een op algoritmen gebaseerd systeem in Oostenrijk blijft werkloze werkzoekenden categoriseren om te bepalen welke steun ze zullen ontvangen van arbeidsbureaus van de overheid.⁶²

28. Veel andere gebieden van de verzorgingsstaat zullen ook worden beïnvloed door nieuwe technologieën die worden gebruikt om risico's te scoren en behoeften te classificeren.⁶³ Hoewel dergelijke benaderingen veel voordelen bieden, is het ook belangrijk om rekening te houden met de problemen die zich kunnen voordoen. Ten eerste komen er veel vragen aan de orde bij het bepalen van de rechten van een individu op basis van voorspellingen die zijn afgeleid van het gedrag van een algemene bevolkingsgroep.⁶⁴ Ten tweede is de werking van de technologieën en hoe ze tot een bepaalde score of classificatie komen vaak geheim, waardoor het is moeilijk vast te houden regeringen en particuliere actoren om zich rekenschap te geven van mogelijke rechtenschendingen.⁶⁵ Ten derde kunnen risicoscoring en categorisering van behoeften bestaande ongelijkheden en discriminatie versterken of verergeren.⁶⁶

F. Communicatie tussen welzijnsinstanties en begunstigden

29. Communicatie die voorheen persoonlijk, telefonisch of per brief plaatsvond, wordt steeds vaker vervangen door online sollicitaties en interacties. Verschillende bijdragen aan de speciale rapporteur noemden problemen met het Universal Credit-systeem in het Verenigd Koninkrijk, waaronder problemen in verband met een gebrek aan internettoegang en/of digitale vaardigheden,⁶⁷ en

⁵⁷ Virginia Eubanks, *Ongelijkheid automatiseren* (2018); Alexandra Chouldechova et. al., 'Een casestudy van door algoritmen ondersteunde besluitvorming bij screeningbeslissingen op hotline voor kindermishandeling', *Proceedings of Machine Learning Research* 81:1–15, 2018; <https://www.nytimes.com/2018/01/02/magazine/can-an-algorithm-tell-when-kids-are-in-danger.html>.

⁵⁸ Philip Gillingham, 'Voorspellende risicomodeller om kindermishandeling te voorkomen: inzichten en implicaties uit Aotearoa/Nieuw-Zeeland', *Journal of Public Child Welfare* (Vol. 11, 2017), p. 150.

⁵⁹ <https://www.theguardian.com/society/2018/sep/16/councils-use-377000-peoples-data-in-efforts-to-predict-child-abuse>; <https://www.communitycare.co.uk/2019/06/14/county-becomes-latest-authority-trial-predictive-algorithms-childrens-social-work/>.

⁶⁰ <https://foreignpolicy.com/2018/12/25/the-welfare-state-is-committing-suicide-by-artificial-intelligence/>.

⁶¹ Pools Hooggerechtshof, zaak K 53/16, 6 juni 2018, <http://trybunal.gov.pl/postepowanie-i-orzeczenia/komunikaty-prasowe/komunikaty-po/art/10168-zarzadzanie-pomoca-kierowana-do-osob-bezrobotnych>.

⁶² EpicenterWorks, op <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/EpicenterWorks.pdf>

⁶³ Zie bijvoorbeeld Data Justice Lab, 'Data Scores as Governance: Investigating use of citizen scoring in public services', december 2018.

⁶⁴ Universiteit van Queensland, op https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/University_of_Queensland.pdf; en Data Justice Lab, op <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/UniversityCardiff.pdf> ("Gegevens op huishoudensniveau en op individueel niveau berusten op een fundamentele personalisering van risico's, waarbij risicofactoren aan individuele kenmerken en gedragingen die ertoe kunnen leiden dat individuele reacties op sociale problemen worden bevoorrecht boven collectieve en structurele reacties, zoals kwesties van ongelijkheid, armoede of racisme.").

⁶⁵ London School of Economics and Political Science, op <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/LSE.pdf>.

⁶⁶ "Maar menselijke vooringenomenheid is ingebouwd in het voorspellende risicomodel." <https://www.wired.com/story/excerpt-from-automating-inequality/>.

⁶⁷ Scottish Council for Voluntary Organisations, at <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/ScottishCouncilVoluntaryOrga> afspraken.pdf; en Citizens Advice Scotland, at

de mate waarin onlineportalen verwarring kunnen zaaien en juridische beslissingen kunnen vertroebelen, waardoor het recht van eisers wordt ondermijnd om beslissingen die hun sociale rechten aantasten te begrijpen en in beroep te gaan.⁶⁸ Soortgelijke kwesties werden ook aan de orde gesteld met betrekking tot andere landen, waaronder Australië⁶⁹ en Griekenland.⁷⁰

30. Een ander probleem is de kans dat als het hele proces van aanvraag en behoud van uitkeringen online is gezet, de situatie uitnodigt tot verdere digitale innovatie. In 2018 moest Zweden een complex digitaal systeem dat door de arbeidsbemiddelingsdienst werd gebruikt om met werkzoekenden te communiceren, terugdraaien vanwege problemen die ertoe leidden dat maar liefst 15% van de beslissingen van het systeem waarschijnlijk onjuist waren.⁷¹

31. Het Targeted Compliance Framework (TCF) van Australië vereist dat werkzoekenden communiceren met een digitaal dashboard om verplichte activiteiten te melden en hun nalevingsstatus te controleren.

Het niet nakomen van een 'wederzijdse verplichting' kan automatisch, zonder tussenkomst van een menselijke beslisser, leiden tot surseance van betaling of het opleggen van geldboetes.

In de inzendingen zijn problemen aan het licht gekomen die te wijten zijn aan een gebrek aan internettoegang en digitale geletterdheid, aan de rigiditeit van een geautomatiseerd systeem dat geen rekening houdt met situaties uit het echte leven.⁷²

III. Digitale technologieën laten werken voor sociale bescherming

Digitale technologieën, waaronder kunstmatige intelligentie, hebben een enorm potentieel om de vele voordelen te bevorderen die consequent worden genoemd door hun voorstanders. Ze doen dit al voor degenen die economisch zeker zijn en het zich kunnen veroorloven om voor de nieuwe diensten te betalen. Ze zouden ook een enorm positief verschil kunnen maken bij het verbeteren van het welzijn van de minder bedeelde leden van de samenleving, maar daarvoor zijn ingrijpende veranderingen in het bestaande beleid nodig. De leidende rol bij een dergelijke inspanning zal door regeringen moeten worden gespeeld door middel van passend fiscaal beleid en stimuleringsmaatregelen, regelgevingsinitiatieven en een oprechte toewijding om de digitale verzorgingsstaat te ontwerpen, niet als een Trojaans paard voor neoliberale vijandigheid tegenover welvaart en regelgeving, maar als een manier om iedereen in de samenleving een behoorlijke levensstandaard te garanderen.

33. Dit rapport heeft getracht problemen aan het licht te brengen die specifiek zijn voor de manieren waarop de digitale verzorgingsstaat is bedacht en geïmplementeerd. Maar veel van de veranderingen die nodig zijn om een digitale dystopie te voorkomen, zullen breder moeten reiken. In zijn toespraak tot de Algemene Vergadering op 24 september 2019 waarschuwde de premier van het Verenigd Koninkrijk voor de gevaren van het digitale tijdperk en wees hij op: (i) het risico van '24 uur per dag toezicht'; (ii) de gevaren van algoritmische besluitvorming; (iii) de moeilijkheid om in beroep te gaan tegen computergegenereerde vaststellingen; en (iv) het onvermogen om verzachtende omstandigheden aan te voeren wanneer de beslisser een algoritme is. Hij besloot nogal onheilspellend door te suggereren dat "[d]igitaal autoritarisme ... een opkomende realiteit is."

73

34. Zijn opmerkingen resoneren sterk in de context van de digitale verzorgingsstaat, ook in relatie tot het Universal Credit-systeem in het Verenigd Koninkrijk. Er is geen magisch recept voor

https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/ChildPovertyActionsGroup_1.pdf.

⁶⁸ Actiegroep Kinderarmoede, 'Computer Says No!', mei 2019, verkrijgbaar bij:

https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/ChildPovertyActionsGroup_2.pdf.

⁶⁹ Senate Community Affairs References Committee, Parliament of Australia, *ontwerp, reikwijdte, kosten-batenanalyse, gegunde contracten en implementatie in verband met het Better Management of the Social Welfare System Initiative* (juni 2017), p. 60.

⁷⁰ Indiening bij de speciale rapporteur door de regering van Griekenland.

⁷¹ AlgorithmWatch, 'Zweden: Rogue-algoritme stopt sociale uitkeringen voor maximaal 70.000 werklozen', 19 februari 2019.

⁷² Mensenrechtencentrum, op

<https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/HumanRightsLawCentre.pdf>; en <https://www.nssrn.org.au/social-security-rights-review/the-targeted-compliance-framework-implications-for-job-seekers/>.

⁷³ <https://www.gov.uk/government/speeches/pm-speech-to-the-un-general-assembly-24-september-2019>.

de valkuilen vermijden waarvoor hij waarschuwde, maar de volgende stappen zouden kunnen helpen om van de digitale verzorgingsstaat een kracht te maken die mensenrechten verbetert in plaats van ondermijnt.

A. Mensenrechten serieus nemen en dienovereenkomstig reguleren

35. De premier van het Verenigd Koninkrijk sloot zijn toespraak af met de waarschuwing dat "[u]ntenzij we ervoor zorgen dat nieuwe technologie" de mensenrechten weerspiegelt, de Universele Verklaring van de Rechten van de Mens "niets zal betekenen...." ⁷⁴ Maar de realiteit is dat overheden de tech-industrie zeker niet hebben gereguleerd alsof mensenrechten op het spel staan, en dat de technologiesector vrijwel een mensenrechtenvrije zone blijft. De Big Tech-bedrijven en hun overheidsondersteuners hebben hard gewerkt om dat zo te houden. Hun aanpak kan voor huidige doeleinden worden samengevat in vier stellingen.

36. De eerste is dat het vermogen om te innoveren vrijheid vereist, vooral van regulering. De vroege oproep van de Facebook-oprichter aan de industrie om "snel te handelen en dingen kapot te maken" illustreert het belang dat wordt gehecht aan het minimaliseren van wettelijke en overheidsbeperkingen. Toch leidt dit argument er onverbiddelijk toe dat een handvol machtige leidinggevenden regeringen en wetgevers vervangen bij het bepalen van de richtingen waarin samenlevingen zullen evolueren en de waarden en veronderstellingen die deze ontwikkelingen zullen sturen. De accumulatie van enorme hoeveelheden kapitaal in de handen van zeer kleine elites en de snelle groei van extreme ongelijkheid zijn tot nu toe hand in hand gegaan met de opkomst van deze benadering.⁷⁵

37. De tweede stelling is dat er geen universele waarden zijn. In een recent boek vroeg de president van Microsoft zich retorisch af: "Hoe kan de wereld het eens worden over een unieke benadering van ethiek voor computers als ze het niet eens kan worden over filosofische kwesties voor mensen?"⁷⁶ Zelfs non-discriminatie-normen worden soms gepresenteerd als te vaag en te omstreven om bruikbaar te zijn bij het reguleren van AI.⁷⁷ Maar deze argumenten zijn egoïstisch en slecht geïnformeerd. Overheden over de hele wereld hebben universele mensenrechtennormen aanvaard, ook in de vorm van bindende wettelijke verplichtingen. En in de afgelopen halve eeuw of langer zijn deze normen uitputtend ontwikkeld en toegepast door rechtbanken en een breed scala aan deskundige en gemeenschapsinstanties. Er blijft voldoende ruimte voor filosofische meningsverschillen, maar er is geen gebrek aan overeenstemming over menselijke kernwaarden.

38. De derde stelling is dat regeringen van nature traag en onhandig zijn en eerder geneigd zijn te reageren op de uitdagingen van gisteren dan op die van morgen. Zoals de Republikeinse minderheidsleider van het Huis van Afgevaardigden van de Verenigde Staten onlangs betoogde: "de bureaucratische leviathan [heeft niet] wat nodig is om behendige reacties op snelle veranderingen in de technologie-industrie te ontwikkelen of af te dwingen." naar voren gebracht door de voorstanders van onbeperkte discretie voor de financiële, luchtvaart-, defensie-, farmaceutische en andere industrieën, is het uitsluitend met betrekking tot Big Tech dat regeringen bereid zijn hun regelgevende verantwoordelijkheden op te geven en in te stemmen met een zelfregulerende benadering van dergelijke een extreme mate. Er is geen rechtvaardiging voor een dergelijk exceptionisme en er is geen empirisch bewijs om de bewering te ondersteunen dat er een fundamentele onverenigbaarheid bestaat tussen innovatie en regelgeving.

39. En de vierde stelling is dat publieke verantwoording niet nodig is omdat de vrije markt de beste regulator is.⁷⁹ Afgezien van de krachtige argumenten dat Big Tech

⁷⁴ idd.

⁷⁵ Zie algemeen Shoshana Zuboff, *The Age of Surveillance Capitalism* (2019); en Emmanuel Saez en Gabriel Zucman, *The Triumph of Injustice: hoe de rijken belastingen ontwijken en hoe ze ervoor zorgen dat ze betalen* (2019).

⁷⁶ Brad Smith en Carol Ann Browne, *Tools and Weapons: The Promise and the Peril of the Digital Leef tijd* (2019), p. 207.

⁷⁷ *Openbare controle van geautomatiseerde beslissingen: vroege lessen en opkomende methoden, een ervaring en Omidyar-netwerkrapport* (2018), p. 25, en n. 115 op https://www.omidyar.com/sites/default/files/file_archive/Public%20Scrutiny%20of%20Automated%20Beslissingen.pdf.

⁷⁸ Kevin McCarthy, 'Reken niet op de overheid om uw privacy te beschermen', *New York Times*, 14 juni 2019.

⁷⁹ Zie in het algemeen Julie Cohen, 'Law for the Platform Economy', *51 UC Davis L. Rev.* 133 (2017).

De grote schandalen van de afgelopen jaren die tot de zogenaamde 'techlash' hebben geleid, zijn zeer concurrentiebeperkend en dus immuun voor vele stromingen van de vrije markt, en leveren overtuigend bewijs dat publieke verantwoording onontbeerlijk is.

40. Als antwoord op de groeiende roep om doeltreffende overheidsregulering, is de industrie in een hogere versnelling gekomen bij het produceren, beïnvloeden en omarmen van 'ethische codes' en andere niet-bindende normen die bedoeld zijn om digitale technologieën en hun ontwikkelaars te 'reguleren'.⁸⁰ De meeste, maar lang niet alle codes bevatten een verwijzing naar mensenrechten, maar de inhoud van mensenrechtenwetgeving ontbreekt stevast. In plaats daarvan dient de symbolische verwijzing naar mensenrechten alleen maar om aanspraken op legitimiteit en universaliteit te versterken. Ondertussen zijn de relevante discussies over ethiek gebaseerd op bijna volledig open begrippen die niet noodzakelijkerwijs gebaseerd zijn op juridische of zelfs filosofische argumenten, en kunnen worden gevormd om te voldoen aan de behoeften van de industrie. Als gevolg hiervan zijn er ernstige problemen van conceptuele incoherentie, worden conflicten tussen normen zelden erkend, wordt zelden zinvolle input gevraagd van belanghebbenden en zijn verantwoordingsmechanismen afwezig.⁸¹ Zelfs ethici die werkzaam zijn in de industrie erkennen dat binnen de logica van marktfundamentalisme, meritocratie en technologisch solutionisme is het onwaarschijnlijk dat de technologiesector een zinvol antwoord zal kunnen bieden op het verlangen naar een meer rechtvaardig en waardengedreven technologie-ecosysteem.⁸² Tegen deze achtergrond is het niet verwonderlijk dat er weinig publieke of wetenschappelijke discussies zijn over de *mensenrechten* implicaties van digitale verzorgingsstaten.

41. De mensenrechtengemeenschap heeft tot nu toe zeer slecht werk geleverd door de industrie, de overheid of schijnbaar de samenleving als geheel te overtuigen van het feit dat een technologisch gedreven toekomst rampzalig zal zijn als deze niet wordt geleid door respect voor de mensenrechten, dat is op zijn beurt gegrond in de wet.

B. Zorgen voor legaliteit en transparantie

42. Een van de meest verrassende kenmerken van te veel belangrijke digitale verzorgingsstaatinitiatieven is een gebrek aan aandacht voor het belang van het waarborgen van legaliteit. Vele voorbeelden zijn onder de aandacht van de Speciale Rapporteur gebracht, waaronder: het online compliance-interventiesysteem van de Australische regering dat geautomatiseerde data-matching gebruikte als basis voor het versturen van grote aantallen schuldbekentenissen met zeer hoge foutenpercentages (bekend als Robodebt);⁸³ vermeend onrechtmatige informatieverstrekking aan eisers via het online Universal Credit-portaal in het Verenigd Koninkrijk;⁸⁴ de betwiste rechtmatigheid van de Irish Public Services Card voor een aantal van de doeleinden waarvoor deze is gebruikt;⁸⁵ het SyRI-systeem (System Risk Indication) in de

⁸⁰ Deze omvatten industriestandaarden, initiatieven van het maatschappelijk middenveld en publieke kaders. Om een paar voorbeelden te geven: IBM, 'Everyday Ethics for Artificial Intelligence' (september 2018); Google, 'AI-principes' (2019); Microsoft, *de toekomst berekend* (2018); IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems; SIIA, 'Ethische principes voor kunstmatige intelligentie en data-analyse' (2017); Asilomar AI-principes (2017); Onafhankelijke deskundigengroep op hoog niveau inzake kunstmatige intelligentie, opgericht door de Europese Commissie, 'Ethics Guidelines for Trustworthy AI' (april 2019).

⁸¹ Karen Yeung, Andrew Howes en Ganna Pogrebna, 'AI Governance by Human Rights-Centred Design, Deliberation and Oversight: An End to Ethics Washing', verschenen in M Dubber en F Pasquale (eds.), *The Oxford Handbook of AI Ethics* (2019), op <https://ssrn.com/abstract=3435011>, p. 22.

⁸² Jacob Metcalf, Emanuel Moss en Danah Boyd [sic], 'Owning Ethics: Corporate Logics, Silicon Valley, and the Institutionalization of Ethics', 82 *Social Research* (2019) 449, op 473.

⁸³ Terry Carney, 'De nieuwe digitale toekomst voor welzijn: schulden zonder wettelijk bewijs of morele autoriteit?', *UNSW Law Journal Forum* (maart 2018).

⁸⁴ https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/ChildPovertyActionsGroep_1.pdf.

⁸⁵ Definitief Onderzoeksrapport: 'Een onderzoek door de Commissie Gegevensbescherming naar de verwerking van persoonsgegevens door de Directie Werkgelegenheid en Sociale Bescherming in het kader van de Publieke Dienstverleningskaart ("PSC") naar de naleving van de verplichtingen met betrekking tot Rechtsgrondslag en transparantie' (2019), op <https://www.welfare.ie/en/pdf/pr170919.pdf>.

Nederland, dat aanvankelijk geen wettelijke basis had en onderwerp blijft van gerechtelijke aanvechting;⁸⁶ en het Aadhaar-systeem in India dat oorspronkelijk zonder wettelijk kader werd geïmplementeerd.⁸⁷

43. Hoewel het ontbreken van een rechtsgrondslag op zich zeer problematisch is, betekent deze leemte ook dat er geen mogelijkheden zijn voor wetgevingsdebatten en voor inbreng van het publiek bij het vormgeven van de relevante systemen. Dit heeft potentieel grote negatieve implicaties voor de transparantie, het ontwerp, de legitimiteit en de kans op acceptatie.

C. Bevordering van digitale gelijkheid

44. Egalitarisme is een consistent thema van de technologie-industrie, zoals blijkt uit het doel van Facebook "om mensen de kracht te geven om een gemeenschap op te bouwen en de wereld dichter bij elkaar te brengen".⁸⁸ Maar op macroniveau is Big Tech een aanjager geweest van groeiende ongelijkheid⁸⁹ en heeft de vorming van een 'enorme digitale onderklasse' mogelijk gemaakt. ⁹⁰

45. De digitale verzorgingsstaat van zijn kant geeft begunstigden soms de keuze om digitaal te gaan of meer traditionele technieken te blijven gebruiken. Maar in werkelijkheid wordt beleid als 'digital by default' of 'digital by choice' in de praktijk meestal omgevormd tot 'digital only'. Dit verergert of creëert op zijn beurt grote verschillen tussen verschillende groepen. Een gebrek aan digitale geletterdheid leidt tot het onvermogen om digitale basishulpmiddelen überhaupt te gebruiken, laat staan effectief en efficiënt. Beperkte of geen toegang tot het internet stelt heel veel mensen voor grote problemen. Er ontstaan extra belemmeringen voor personen die hoge prijzen moeten betalen om internettoegang te krijgen, om lange afstanden af te leggen of daarvoor afwezig te zijn van hun werk, om openbare voorzieningen zoals bibliotheken te bezoeken om toegang te krijgen, of om hulp te krijgen van personeel of vrienden om te navigeren de systemen. En hoewel de welgestelden direct toegang hebben tot up-to-date en gebruiksvriendelijke computers en andere hardware, evenals snelle en efficiënte breedbandsnelheden, lopen de minst bedeelden veel meer kans ernstig benadeeld te worden door data-apparatuur en tijdrovende en onbetrouwbare digitale verbindingen.

46. Inzendingen aan de speciale rapporteur uit een groot aantal landen benadrukten het belang van deze verschillende problemen. Zowel in het Globale Noorden als in het Globale Zuiden hebben veel individuen, en vooral degenen die in armoede leven, thuis geen betrouwbare internetverbinding, kunnen zich zo'n verbinding niet veroorloven,⁹² zijn niet digitaal vaardig of zelfverzekerd,⁹³ of zijn anderszins geremd in online communiceren met autoriteiten. De verschillende zienswijzen benadrukken hoe deze problemen het vermogen van aspirant-gerechtigden belemmeren om hun mensenrechten te realiseren.

⁸⁶ Brief van de Speciale Rapporteur van de Verenigde Naties inzake extreme armoede en mensenrechten als Amicus Curiae in de zaak NJCM cs/De Staat der Nederlanden (SyRI) voor de Rechtbank Den Haag (zaaknummer: C/09/550982/HA ZA 18/388) (september 2019), op <https://www.ohchr.org/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf>.

⁸⁷ Indiening bij de speciale rapporteur door National Law University Delhi, verkrijgbaar bij: <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/NationalLawUniversityDelhi.pdf>.

⁸⁸ Kevin Munger, 'De opkomst en ondergang van de Palo Alto-consensus', *New York Times*, 10 juni 2019.

⁸⁹ Isobel Asher Hamilton, 'A definitieve lijst van de 13 rijkste tech miljardairs ter wereld', *Business Insider*, 9 maart 2019, beschikbaar via: <https://www.businessinsider.nl/net-worth-13-richest-tech-miljardairs-in-de-wereld-2019-3?international=true&r=US>.

⁹⁰ Farhad Manjoo, 'De technische industrie bouwt aan een enorme digitale onderklasse', *The New York Times*, 24 juli 2019.

⁹¹ <https://www.wired.com/story/global-internet-access-dire-reports/>; <https://data.oecd.org/ict/internetaccess.htm>; <https://www.oecd.org/internet/oecd-toolkit-aims-to-spur-high-speed-internet-use-in-latin-america-and-the-caribbean.htm>.

⁹² https://a4ai.org/affordability-report/report/2018/#2018:_where_are_we_on_the_road_to_affordable_universal_internet_access?; <https://webfoundation.org/2019/03/new-mobile-broadband-pricing-data-reveals-stalling-progress-on-betalbaarheid/>; In de Verenigde Staten gebruikt 27% van de bevolking thuis geen snel breedbandinternet, en dat cijfer loopt op tot 44% voor mensen met een inkomen van minder dan \$30.000: <https://www.pewinternet.org/fact-blad/internet-breedband/>.

⁹³ Europese Commissie, 'Human Capital: Digital Inclusion and Skills' (2019).

47. Het Verenigd Koninkrijk geeft een voorbeeld van een welvarend land waar, zelfs in 2019, 11,9 miljoen mensen (22% van de bevolking) niet beschikken over de 'essentiële digitale vaardigheden' die nodig zijn voor het dagelijks leven. Nog eens 19% kan fundamentele taken niet uitvoeren, zoals het aanzetten van een apparaat of het openen van een app. Daarnaast zijn 4,1 miljoen volwassenen (8%) offline vanwege de angst dat het internet een onveilige omgeving is, en verhoudingsgewijs komt bijna de helft daarvan uit een huishouden met een laag inkomen en bijna de helft is jonger dan zestig jaar.⁹⁴

48. Deze problemen worden nog verergerd door het feit dat wanneer digitale technologieën worden geïntroduceerd in verzorgingsstaten, hun verdelende effect vaak geen significante focus is van regeringen.⁹⁵ Bovendien worden kwetsbare individuen gewoonlijk niet betrokken bij de ontwikkeling van IT-systemen en de IT-systemen. professionals zijn vaak slecht toegerust om te anticiperen op het soort problemen dat zich waarschijnlijk zal voordoen.⁹⁶ Programma's gaan er vaak zonder rechtvaardiging van uit dat individuen gemakkelijk toegang hebben tot officiële documenten en deze kunnen uploaden, dat ze een kredietgeschiedenis of bredere digitale financiële voetafdruk, of zelfs dat hun vingerafdrukken leesbaar zullen zijn, wat vaak niet het geval is voor degenen wier beroepsleven gepaard ging met niet-aflatende handarbeid.

49. Wat het digitale welzijnsbeleid betreft, komen verschillende conclusies naar voren. Ten eerste moet er altijd een echte niet-digitale optie beschikbaar zijn.⁹⁷ Ten tweede moeten programma's die gericht zijn op het digitaliseren van welzijnsarrangementen vergezeld gaan van programma's die zijn ontworpen om de benodigde digitale vaardigheden te bevorderen en aan te leren en om te zorgen voor een redelijke toegang tot de benodigde apparatuur en effectieve online toegang. Ten derde, om de schade die wordt veroorzaakt door onjuiste aannames en verkeerde ontwerpkeuzes te verminderen, moeten digitale socialezekerheidsstelsels mede worden ontworpen door de beoogde gebruikers en op participatieve wijze worden geëvalueerd.

D. Bescherming van economische en sociale rechten in de digitale verzorgingsstaat

50. De processen van digitalisering en de toenemende rol van geautomatiseerde besluitvorming door het gebruik van algoritmen en kunstmatige intelligentie hebben, in ieder geval in sommige opzichten, geleid tot een verschuiving naar een bureaucratisch proces, weg van een proces dat gebaseerd is op het recht op sociale zekerheid of het recht op sociale bescherming. In plaats van het ideaal dat de staat verantwoording aflegt aan de burger om ervoor te zorgen dat deze een behoorlijke levensstandaard kan genieten, is de verantwoordingsplicht in veel opzichten omgekeerd. Meer dan in het verleden vaak het geval was, berust de huidige digitale verzorgingsstaat vaak op de uitgangspunten dat het individu geen rechthebbende is maar een aanvrager. In die hoedanigheid moet een persoon de beslisser ervan overtuigen dat hij 'verdiend' is, dat hij voldoet aan de geschiktheidscriteria, dat hij heeft voldaan aan de vaak zware voorgeschreven verplichtingen en dat hij geen andere middelen van bestaan heeft. En veel hiervan moet elektronisch worden gedaan, ongeacht de vaardigheden van de aanvrager op dat gebied.

51. Het recht op sociale zekerheid⁹⁸ omvat het recht "op toegang tot en behoud van uitkeringen, zowel in geld als in natura, zonder discriminatie".⁹⁹ Het opleggen van technologische

⁹⁴ 'The Digitally Disadvantaged', in *UK Consumer Digital Index 2019 – Belangrijkste bevindingen* (Lloyds Bank 2019).

⁹⁵ <https://www.nytimes.com/2019/04/25/opinion/privacy-poverty.html>.

⁹⁶ Indiening bij de speciale rapporteur door ICTU, verkrijgbaar bij:

<https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/ICTU.pdf>.

⁹⁷ Association for Progressive Communications, Derechos Digitales en Media Matters for Democracy, bij

https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/APC_DrechosDigitalesMedia.pdf; Citizens Advice Scotland, op

<https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/CitizensAdviceScotland.pdf>; National Social Security Rights Network, op [https://](https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/NationalSocialSecurityRightsNetwork.pdf)

www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/NationalSocialSecurityRightsNetwork.pdf.

⁹⁸ Artikel 9 van het Internationaal Verdrag inzake economische, sociale en culturele rechten (ICESCR).

⁹⁹ Comité voor economische, sociale en culturele rechten, Het recht op sociale zekerheid, Algemeen commentaar nr. 19 (2007), para. 2.

vereisten kunnen het voor personen onmogelijk of zeer moeilijk maken om effectief toegang te krijgen tot dat recht, waardoor het feitelijk onbetaalbaar wordt.¹⁰⁰

52. Het recht op sociale bescherming is onlosmakelijk verbonden met wat het Mensenrechtencomité het recht op een waardig leven noemt, dat waar nodig moet worden beschermd door middel van "maatregelen die zijn ontworpen om ervoor te zorgen dat individuen onverwijld toegang hebben tot essentiële goederen en diensten zoals voedsel, water, onderdak, gezondheidszorg, elektriciteit en sanitaire voorzieningen en andere maatregelen ter bevordering en vergemakkelijking van adequate algemene voorwaarden ... "101 Er zijn ook diverse andere rechten bij betrokken, waaronder het recht op een behoorlijke levensstandaard, het recht op geestelijke gezondheid en het recht op een waardige behandeling.

53. Hoewel sociale bescherming in het algemeen ontworpen moet zijn om deze rechten te beschermen, loopt de waardigheidsdimensie een bijzonder risico in de context van de digitale verzorgingsstaat. De potentiële risico's doen zich in verschillende contexten voor. Ten eerste kan het proces om te bepalen of iemand in aanmerking komt gemakkelijk worden omgevormd tot een elektronisch vraag- en antwoordproces dat bijna onvermijdelijk toch al kwetsbare personen nog meer benadeelt. Ten tweede kan de manier waarop vaststellingen worden geformuleerd en gecommuniceerd worden ontmenselijkt en geen ruimte laten voor zinvolle vragen of opheldering.

54. Ten derde lijkt de digitale verzorgingsstaat vaak gepaard te gaan met verschillende vormen van rigiditeit en het robotisch toepassen van regels. Bijgevolg worden verzachtende omstandigheden, zoals te laat komen op een afspraak wegens dringende zorgverplichtingen, of het niet kunnen begrijpen van een schriftelijke communicatie vanwege een handicap of een persoonlijke crisis, vaak niet in aanmerking genomen in een overwegend digitale context. Ten vierde zijn digitale systemen vaak niet ontworpen om snel te reageren op ernstige noodsituaties of op de dagelijkse uitdagingen van een oudere persoon van wie het recht plotseling en op onverklaarbare wijze elektronisch is verminderd of geannuleerd, of van een alleenstaande ouder die niet in staat is om een kind naar een plaatselijk ziekenhuis te brengen. Kinderopvang omdat de digitale identiteitskaart niet werkt.

55. Ten vijfde kunnen de manieren waarop diensten worden verleend gemakkelijk vernederende connotaties hebben, zoals het onnodig blootstellen aan een breder publiek van het feit dat een persoon afhankelijk is van een uitkering, of het eisen van lange wachttijden, of het navigeren door lange wachtrijen. Ten zesde kan de introductie van verschillende nieuwe technologieën die de menselijke leverancier elimineren, de efficiëntie verbeteren en andere voordelen bieden, maar hoeft niet noodzakelijkerwijs bevredigend te zijn voor personen die zich in bijzonder kwetsbare situaties bevinden. Nieuwe technologieën werken vaak volgens de wet van gemiddelden, in het belang van meerderheden en op basis van voorspelde uitkomsten of waarschijnlijkheden.

56. Ten zesde bestaat het risico dat digitale diensten een groot deel van de menselijke interactie en mededogen, die waarschijnlijk onmisbare componenten zullen zijn om in ieder geval een aantal uitkeringsgerechtigden de zorg en hulp te bieden die ze nodig hebben, vrijwel geheel uitsluiten. De veronderstelling dat er altijd een technologische oplossing is voor elk probleem, is hoogstwaarschijnlijk misplaatst in verschillende aspecten van een humaan en effectief systeem van sociale bescherming.

E. Bescherming van burgerrechten en politieke rechten in de digitale verzorgingsstaat

57. Dat de armen te lijden hebben onder intensievere controles, controles en bewaking, is nauwelijks een originele observatie. In de jaren zestig schreef Charles Reich dat uitkeringsgerechtigden in de Verenigde Staten "onderworpen zijn aan vele vormen van procedures en controles die niet aan andere burgers zijn opgelegd. ... [Ze] zijn maar al te gemakkelijk te reguleren."¹⁰² In 1975 schreef Michel Foucault over de 'dwingende gedragstechnologieën' die in de moderne samenleving worden gebruikt om de armere klassen te 'disciplineren en te straffen'.¹⁰³

58. Om uit te leggen waarom deze lessen niet zijn geleerd in de digitale verzorgingsstaat, schrijft Shoshana Zuboff dat het systeem van 'toezichtkapitalisme' dat tegenwoordig heerst

¹⁰⁰ Id, alinea's. 24-27.

¹⁰¹ Mensenrechtencomité, algemeen commentaar nr. 36 (2018) op artikel 6 van het Internationaal Verdrag inzake burgerrechten en politieke rechten, over het recht op leven, para. 26.

¹⁰² Charles A. Reich, 'Individuele rechten en sociaal welzijn: de opkomende juridische kwesties', 74 *Yale LJ* (1965), blz. 1245.

¹⁰³ Michel Foucault, *Discipline en straf: de geboorte van de gevangenis* (1991), p. 222.

is ongekend, wat "het mogelijk heeft gemaakt om systematische strijd te ontwijken omdat het niet adequaat kan worden begrepen met onze bestaande concepten."¹⁰⁴ Dit privétoezicht wordt versterkt door trends in overheidsstoezicht. Jack Balkin heeft de 'National Surveillance State' beschreven als 'een permanent kenmerk van bestuur [dat] na verloop van tijd net zo alomtegenwoordig zal worden als de bekende apparaten van de regelgevende en verzorgingsstaten'.¹⁰⁵

59. In de verzorgingsstaat worden digitale technologieën gebruikt om begunstigden, met name de armste en meest kwetsbaren onder hen, te bewaken, aan te vallen, lastig te vallen en te straffen. Nogmaals, veel van de inzendingen die de speciale rapporteur heeft ontvangen, dienen om dit punt te illustreren en te versterken. Ze dienen om een aantal mensenrechtenkwesties onder de aandacht te brengen. Ten eerste bestaat er in de context van socialezekerheidsuitkeringen en -bijstand een reëel risico dat begunstigden effectief worden gedwongen om hun recht op privacy en gegevensbescherming op te geven om hun recht op sociale zekerheid en andere sociale rechten te ontvangen.¹⁰⁶

60. Een tweede punt van zorg is de vervaging van de scheidslijn tussen openbaar en particulier toezicht. De autoriteiten van de verzorgingsstaat vertrouwen steeds meer, actief of passief, op particuliere ondernemingen voor het toezicht op en het richten van begunstigden. Particuliere entiteiten hebben verschillende motieven voor hun betrokkenheid bij uitkerings- en bijstandsstelsels en dit kan leiden tot conflicten tussen de publieke belangen die deze stelsels dienen te dienen en de particuliere belangen van ondernemingen en hun eigenaren.

61. Een derde punt van zorg is het potentieel voor opzettelijke aanvallen op en intimidatie van de armen door middel van nieuwe technologieën in de verzorgingsstaat. Zoals een inzending aan de speciale rapporteur benadrukt, is fraude in de verzorgingsstaat vaak het resultaat van verwarring, complexiteit en het onvermogen om de resulterende fouten te corrigeren.¹⁰⁷ Maar door opzettelijk de kracht van nieuwe technologieën te gebruiken om fraude of schendingen van 'voorwaarden' te identificeren opgelegd aan begunstigden, zullen regeringen waarschijnlijk inconsistenties ontdekken die zij eisers kunnen verwijten. Het is hier relevant dat nieuwe technologieën mogelijk maken wat Jack Balkin omschreef als de 'dood van geheugenverlies': nieuwe mogelijkheden om informatie te verzamelen en deze voor onbepaalde tijd digitaal op te slaan, creëren een toekomst waarin een schat aan informatie tegen iemand kan worden gebruikt voor onbepaalde tijd.¹⁰⁸

62. Bijkomende zorgen die meer aandacht verdienen dan in dit rapport kan worden vermeld, zijn onder meer (i) de gevolgen voor de mensenrechten van de overstap naar het voorspellen van risico's in plaats van het achteraf handhaven van regelovertredingen;¹⁰⁹ (ii) de gevaren van het verbinden van overheidsgegevenssilos, die in de welzijnscontext gemakkelijker worden overwogen dan elders op het gebied van digitaal bestuur;¹¹⁰ (iii) de psychologische en maatschappelijke kosten van voortdurende monitoring en toezicht;¹¹¹ en (iv) de groeiende neiging van sommige regeringen om de mogelijkheden van de digitale verzorgingsstaat te gebruiken om te proberen sociaal gedrag te veranderen, hetzij in de vorm van seksuele activiteit of voorkeuren, benaderingen van samenwonen, het gebruik van alcohol of drugs, de beslissing om kinderen te krijgen, of vele andere soortgelijke doelen.¹¹²

104 Shoshana Zuboff, *The Age of Surveillance Capitalism* (2019), p. 14.

105 Jack Balkin, 'De grondwet in de National Surveillance State', *Minnesota Law Review* (Vol. 93, 2008), p. 1-18.

106 Indiening bij de speciale rapporteur door de regering van Mexico; Verklaring over bezoek aan de VS, door professor Philip Alston, speciale rapporteur van de Verenigde Naties voor extreme armoede en mensenrechten, 15 december 2017, paragraaf 57.

107 Internationaal Verbond van Vakbonden, at <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/ITCU.pdf>.

108 Jack Balkin, 'The Constitution in the National Surveillance State', *Minnesota Law Review* (Vol. 93, 2008), blz. 13.

109 Idd, p. 11.

110 https://www.washingtonpost.com/news/theworldpost/wp/2018/08/09/aadhaar/?utm_term=.8a17992dfb6e.

111 "In ons onderzoek met maatschappelijke groeperingen ... waren zorgen over stigmatisering en het gevoel het doelwit te zijn prominenter aanwezig dan zorgen over privacy op zich." Data Justice Lab, op <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/UniversityCardiff.pdf>.

112 Zie Foucaults analyse van panoptische systemen die "kunnen worden gebruikt als een machine om experimenten uit te voeren, gedrag te veranderen, individuen te trainen en te corrigeren". Michel Foucault, *Discipline en straf: de geboorte van de gevangenis* (1991), p. 203.

F. Weerstand bieden tegen de onvermijdelijkheid van een toekomst die alleen digitaal is

63. Digitale technologieën in het algemeen, en in het bijzonder de technologieën die centraal staan in de digitale verzorgingsstaat, worden vaak gepresenteerd als zowel onvermijdelijk als onweerstaanbaar. Als een land gezien wil worden als technologisch toonaangevend, als de regering het meest efficiënte, economische en flexibele socialezekerheidsstelsel wil hebben, en als de burgers al het gemak willen dat voortkomt uit het niet hoeven overleggen van een identiteitsbewijs in Om verschillende transacties te kunnen doen, moet een transitie naar een digitale verzorgingsstaat worden nagestreefd. Maar afgezien van de keuzes die burgers en overheden zouden kunnen maken als ze volledig geïnformeerd en adequaat geraadpleegd zouden zijn, is de realiteit dat dergelijke beslissingen maar al te vaak worden genomen zonder geavanceerde kosten-batenanalyses. En wanneer dergelijke analyses worden uitgevoerd, bestaan ze uit financiële balansen die voorbijgaan aan wat men de fiscaal onzichtbare immateriële activa zou kunnen noemen die ten grondslag liggen aan mensenrechten. Waarden als waardigheid, keuzevrijheid, zelfrespect, autonomie, zelfbeschikking, privacy en een reeks andere factoren worden allemaal verhandeld zonder dat ze in de algemene vergelijking worden meegenomen, alles behalve dat er gegarandeerd wordt dat er onvoldoende stappen zullen worden genomen om hun rol in de nieuwe digitale systemen.

64. Vaak wordt aangenomen dat ten minste enkele van deze compromissen kunnen worden gerechtvaardigd op grond van het feit dat de overeenkomst slechts een zaak is tussen het individu en een bepaalde overheidsinstantie. Maar zo'n beeld is steeds verder verwijderd van de waarheid, aangezien kruisvergelijking, het delen van gegevens en kruisverificatie systematisch de pools van gegevens vergroten die mogelijk beschikbaar zijn over het hele spectrum van de overheid. Voor zover er garanties worden gegeven dat er geen lekkage van de ene silo naar de volgende zal plaatsvinden, zijn dergelijke garanties grotendeels illusoir, aangezien een regeringswisseling of een echte of ingebeeldde noodsituatie het enige is dat nodig is om een gedeeltelijke of algehele uitval van het systeem teweeg te brengen. de partities, afgezien van de risico's van elektronische datalekken als gevolg van hacking of normale systeemstoringen. Daarnaast is de aanname dat het alleen een relatie tussen overheid en burger is ook anachronistisch. Bedrijfsfactoren zijn nu centraal betrokken bij grote delen van het socialezekerheidsstelsel, en in combinatie met het steeds groter wordende bereik van andere vormen van surveillancekapitalisme kan worden aangenomen dat immateriële mensenrechtenwaarden evenveel waard zijn als de aandelen van een failliete onderneming.

65. De Speciale Rapporteur heeft kennis genomen van situaties waarin cruciale beslissingen om digitaal te gaan zonder overleg zijn genomen door ministers van de regering, of zelfs door departementale ambtenaren zonder dat er belangrijke beleidsdiscussies hebben plaatsgevonden, omdat de verhuizing in wezen een administratieve aangelegenheid is, in plaats van een potentieel baanbrekende benadering te betrekken bij een groot deel van het officiële beleid. Soms lijkt het vermoeden te bestaan dat zelfs als de overstap naar digitaal momenteel niet nodig is, het op een dag zeker zal gebeuren en dat het beter is om van tevoren over te stappen. Steun voor dergelijke preventieve maatregelen kan afkomstig zijn van bedrijfsbelangen, maar ook van de veiligheids- en terrorismebestrijdingssectoren, zij het om geheel andere redenen. Er moet altijd zorgvuldig en transparant worden nagedacht over de vraag waarom, voor wie, wanneer en hoe transitie naar digitale systemen plaatsvinden.

66. En zelfs als er gedetailleerde kostenramingen worden verstrekt, is dit een gebied waarop nauwkeurigheid moeilijk te bereiken lijkt. Helen Margetts heeft bijvoorbeeld opgemerkt dat in het Verenigd Koninkrijk "[t]echnologie en de publieke sector zelden gelukkige bedgenoten zijn geweest" en "elk technologieproject van de overheid gedoemd lijkt te laat aan te komen, ondermaats te presteren en het budget te overschrijden."¹¹³ Een ander voorbeeld is het Aadhaar-systeem in India, waarvan wordt gezegd dat het een goede kosten-batenanalyse heeft ontbroken voorafgaand aan implementatie¹¹⁴ en waarover grote onenigheid bestond over de post hoc beoordeling van kosten en baten.¹¹⁵

¹¹³ <https://theconversation.com/back-to-the-bad-old-days-as-civil-service-infighting-threatens-uks-only-hope-for-digital-government-47683>.

¹¹⁴ National Law University Delhi, op <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/NationalLawUniversityDelhi.pdf>.

¹¹⁵ Reetika Khera, 'Een kosten-batenanalyse van UID', *Economic and Political Weekly*, Vol. 48, nr. 5 (2 februari 2013), p. 13-15; <https://www.iisd.org/gsi/subsidy-watch-blog/estimating-impact-indias-aadhaar-scheme-lpg-subsidy-expenditure>; <https://economictimes.indiatimes.com/blogs/et-commentary/aadhaars-11-bn-question/>; <https://thewire.in/economy/the-curious-case-of-the-world->

G. De rol van de particuliere sector

67. Twee consistente thema's van dit rapport zijn de onwil van veel regeringen om de activiteiten van technologiebedrijven te reguleren, en de sterke weerstand van die bedrijven om systematisch rekening te houden met mensenrechtenoverwegingen. Het feit dat dit ertoe leidt dat veel grote technologiebedrijven in een bijna mensenrechtenvrije zone opereren, wordt nog verergerd door de mate waarin de particuliere sector een leidende rol speelt bij het ontwerpen, bouwen en zelfs exploiteren van belangrijke delen van de digitale verzorgingsstaat.¹¹⁶

68. Tot de bekende voorbeelden behoren de betrokkenheid van Net 1-dochteronderneming Cash Paymaster Services (CPS), MasterCard en Grindrod Bank bij de distributie van sociale subsidies gekoppeld aan het biometrische identificatiesysteem van Zuid-Afrika, de rol van Indue en Visa in de Cashless Debit Card proeven in Australië en de betrokkenheid van IBM bij het beheersysteem voor sociale bijstand in Ontario. Bijdragen aan de speciale rapporteur hebben ook de aandacht gevestigd op de toenemende rol van de particuliere sector op de Duitse markt voor software voor openbaar bestuur die wordt gebruikt voor werkloosheidsdiensten, sociale voorzieningen en jeugdzorg;

117 en

uitbesteding door lokale autoriteiten in het Verenigd Koninkrijk aan particuliere bedrijven op het gebied van sociale bescherming.¹¹⁸ Verschillende opmerkingen wijzen daarentegen op de bewuste keuze van de betrokken regeringen om *geen* beroep te doen op particuliere actoren om een sleutelrol in de verzorgingsstaat te spelen.¹¹⁹

69. De speciale rapporteur heeft elders de kwesties besproken die voortkomen uit de privatisering van openbare diensten in meer algemene zin.¹²⁰ Maar met betrekking tot sociale beschermingsdiensten er is een zeer problematisch gebrek aan informatie over de precieze rol en verantwoordelijkheid van particuliere actoren bij het voorstellen, ontwikkelen en gebruiken van digitale technologieën in verzorgingsstaten over de hele wereld. Dit gebrek aan transparantie heeft verschillende oorzaken, van lacunes in wetten op de vrijheid van informatie, vertrouwelijkheidsclausules en bescherming van intellectueel eigendom, het nalaten van wetgevers en uitvoerende machten om transparantie te eisen, tot een algemeen gebrek aan onderzoek naar deze praktijken door toezichthoudende instanties en de media.¹²¹ Het ontbreken van informatie vormt een ernstige belemmering voor het ter verantwoording roepen van overheden en private actoren.

H. Verantwoordingsmechanismen

70. Veel van de programma's die worden gebruikt om de digitale verzorgingsstaat te promoten, zijn ontworpen door dezelfde bedrijven die zich zo sterk verzetten tegen het naleven van mensenrechtennormen. Bovendien wordt er steeds meer op die bedrijven en hun gelieerde ondernemingen vertrouwd om belangrijke onderdelen van de eigenlijke welzijnsprogramma's te ontwerpen en uit te voeren. Het is dus duidelijk dat het uitgangspunt voor inspanningen om te zorgen voor mensenrechtencompatibele digitale verzorgingsstaten, is te zorgen

bank-en-aadhaar-sparen; en <https://qz.com/india/1519209/why-india-cant-cite-world-bank-to-brag-about-aadhaar/>.

¹¹⁶ regering van Ierland, op

<https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/Ireland.pdf>; Regering van Estland, op <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/Estonia.docx>; Indiening bij de speciale rapporteur door de regering van Kroatië.

¹¹⁷ AlgorithmWatch, op

<https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/AlgorithmWatch.pdf>.

¹¹⁸ Data Justice Lab,

op <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/UniversityCardiff.pdf>.

¹¹⁹ Universiteit van Auckland,

op <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/UniversityAuckland.docx>; Indiening bij de speciale rapporteur door de regering van Griekenland; Indiening bij de speciale rapporteur door de regering van Argentinië.

¹²⁰ A/73/396 (2018).

¹²¹ AlgorithmWatch, op

<https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/AlgorithmWatch.pdf>; Privacy International,

op <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/PrivacyInternational.pdf>;

Ierse Raad voor Burgerlijke

Vrijheden, op <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/IrishCouncilCivilLiberties.pdf>.

via overheidsregulering dat technologiebedrijven wettelijk verplicht zijn om toepasselijke internationale mensenrechtenstandaarden te respecteren.¹²²

IV. Conclusies

71. Er is geen gebrek aan analyses die waarschuwen voor de gevaren voor de mensenrechten van verschillende verschijningsvormen van digitale technologie en met name kunstmatige intelligentie. Maar deze studies richten zich overwegend op de traditionele burgerrechten en politieke rechten, zoals het recht op privacy, non-discriminatie, rechten op een eerlijk proces en het recht op vrijheid van meningsuiting en informatie. Op een handvol uitzonderingen na heeft geen enkele de volledige reeks bedreigingen die de opkomst van de digitale verzorgingsstaat met zich meebrengt, voldoende ondervangen. De overgrote meerderheid van de staten geeft zeer grote sommen geld uit aan verschillende vormen van sociale bescherming, of welzijn, en de aantrekkingskracht van digitale systemen die grote kostenbesparingen opleveren, samen met personeelsverminderingen, grotere efficiëntie en vermindering van fraude, om nog maar te zwijgen van de bijbehorende complimenten met de technologische vooruitgang. Het lijkt geen twijfel dat de toekomst van de welvaart integraal verbonden zal zijn met digitalisering en de toepassing van AI.

72. Maar terwijl de mensheid zich, misschien wel onverbiddelijk, beweegt in de richting van de digitale welvaartstoekomst, moet ze aanzienlijk en snel van koers veranderen om te voorkomen dat ze als een zombie in een digitale welvaartsdystopie terechtkomt. Zo'n toekomst zou er een zijn waarin: onbeperkte data-matching wordt gebruikt om de kleinste onregelmatigheden in het dossier van uitkeringsgerechtigden bloot te leggen en te bestraffen (terwijl dergelijke maatregelen met betrekking tot de welgestelden ijverig worden vermeden); steeds verfijndere bewakingsopties maken 24 uur per dag monitoring van begunstigden mogelijk; voorwaarden worden opgelegd aan ontvangers die de individuele autonomie en keuzevrijheid ondermijnen met betrekking tot seksuele en reproductieve keuzes, en met betrekking tot voedsel, alcohol en drugs en veel meer; en zeer bestraffende sancties kunnen worden opgelegd aan degenen die uit de pas lopen.

73. Redelijkerwijs zal worden tegengeworpen dat dit rapport onevenwichtig of eenzijdig is, omdat de aandacht vooral uitgaat naar de risico's en niet naar de vele voordelen die de digitale verzorgingsstaat in potentie kan opleveren. De rechtvaardiging is eenvoudig. Er zijn heel veel cheerleaders die de voordelen ophemelen, maar al te weinig mensen die nuchter nadenken over de nadelen. In plaats van te trachten bovenstaande analyse samen te vatten, zijn een aantal aanvullende opmerkingen op zijn plaats.

74. Ten eerste zijn digitale verzorgingsstaattechnologieën niet het onvermijdelijke resultaat van 'wetenschappelijke' vooruitgang, maar weerspiegelen ze politieke keuzes van mensen. Ervan uitgaande dat technologie vooraf bepaalde of objectief rationele en efficiënte resultaten weerspiegelt, loopt het risico dat mensenrechtenprincipes en democratische besluitvorming worden losgelaten.

75. Ten tweede, als de logica van de markt consequent de overhand krijgt, negeert ze onvermijdelijk mensenrechtenoverwegingen en legt ze "externe zaken op aan de samenleving, bijvoorbeeld wanneer AI-systemen zich bezighouden met vooringenomenheid en discriminatie ... en de menselijke autonomie in toenemende mate verminderen".¹²³

76. Ten derde worden de waarden die de nieuwe technologieën ondersteunen en vormgeven onvermijdelijk vertekend door het feit dat er "een diversiteitscrisis is in de AI-sector over geslacht en ras heen".¹²⁴ Degenen die AI-systemen ontwerpen in het algemeen, evenals degenen die zich richten op de verzorgingsstaat zijn overwegend blank, mannelijk, welvarend en afkomstig uit het mondiale noorden.

¹²² Zie Yeung et al, hierboven; Paul Nemitz, 'Constitutionele democratie en technologie in het tijdperk van kunstmatige intelligentie', *Philosophical Transactions*, A 376 (2018); en Karen Yeung, 'A study of the implicaties van geavanceerde digitale technologieën (inclusief AI-systemen) voor het concept van verantwoordelijkheid binnen een mensenrechtenkader', Raad van Europa doc. MSI-AUT(2018)05 rev (22 mei 2019).

¹²³ Anton Korinek, 'Ethische waarden en economische waarde integreren om vooruitgang in kunstmatig te sturen Intelligentie' (2019) p. 2, op <http://www.nber.org/papers/w26130>.

¹²⁴ Sarah West, Meredith Whittaker en Kate Crawford, *Discriminerende systemen: Gender, Race and Power in AI* (AI Now Institute, 2019) (Vrouwen vormen "15% van het AI-onderzoekspersoneel bij Facebook en 10% bij Google. ... [en] slechts 2,5% van het personeelsbestand van Google is zwart, terwijl Facebook en Microsoft elk 4% zijn.").

Hoe toegewijd ze ook zijn aan bepaalde waarden, de aannames en keuzes die worden gemaakt bij het vormgeven van de digitale verzorgingsstaat zullen bepaalde perspectieven en levenservaringen weerspiegelen. De manier om deze vooroordelen tegen te gaan en ervoor te zorgen dat er voldoende rekening wordt gehouden met mensenrechtenoverwegingen, is ervoor te zorgen dat de "praktijken die ten grondslag liggen aan het creëren, controleren en onderhouden van gegevens" aan zeer zorgvuldig onderzoek worden onderworpen.¹²⁵

77. Ten vierde is het zeer waarschijnlijk dat voorspellende analyses, algoritmen en andere vormen van AI de vooroordelen die in bestaande gegevens en beleid tot uiting komen, reproduceren en verergeren. Ingebouwde vormen van discriminatie kunnen het recht op sociale bescherming van belangrijke groepen en individuen dodelijk ondermijnen. Er moet daarom een gezamenlijke inspanning worden geleverd om dergelijke vooroordelen bij het ontwerpen van de digitale verzorgingsstaat te identificeren en tegen te gaan. Dit vereist op zijn beurt transparantie en een brede inbreng in beleidsvormingsprocessen. Het publiek, en vooral degenen die rechtstreeks door het socialezekerheidsstelsel worden beïnvloed, moet het beleid dat diep in de algoritmen verborgen zit, kunnen begrijpen.

78. Ten vijfde, vooral maar niet alleen in het Globale Noorden, is de technologie-industrie sterk gericht op het ontwerpen en verkopen van gadgets voor de welgestelden, zoals zelfrijdende en vliegende auto's en elektronische persoonlijke assistenten voor multitaskende zakenmensen [sic]. Bij gebrek aan fiscale prikkels, overheidsregulering en politieke druk zal het te weinig aandacht besteden aan het faciliteren van de totstandkoming van een verzorgingsstaat die ten volle rekening houdt met de menselijkheid en zorgen van de minderbedeelden in welke samenleving dan ook.

79. Ten zesde is er tot op heden verbazingwekkend weinig aandacht besteed aan de manieren waarop nieuwe technologieën de verzorgingsstaat ten goede kunnen veranderen. In plaats van geobsedeerd te zijn door fraude, kostenbesparingen, sancties en marktgestuurde definities van efficiëntie, zou het uitgangspunt moeten zijn hoe bestaande of zelfs uitgebreide welzijnsbudgetten door middel van technologie kunnen worden getransformeerd om een hogere levensstandaard voor de kwetsbaren en kansarmen te waarborgen, om nieuwe manieren te bedenken om voor degenen die zijn achtergebleven te zorgen, en effectievere technieken om tegemoet te komen aan de behoeften van degenen die moeite hebben om de arbeidsmarkt te betreden of opnieuw te betreden. Dat zou de echte digitale revolutie van de verzorgingsstaat zijn.

¹²⁵ Rashida Richardson, Jason M. Schultz en Kate Crawford, 'Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice', 94 New York University Law Review (2019) 192, op 225.

Advance Unedited Version

Distr.: General
11 October 2019

Original: English

Seventy-fourth session

Item 72(b) of the provisional agenda*

Promotion and protection of human rights:

**Human rights questions, including alternative approaches
for improving the effective enjoyment of human rights
and fundamental freedoms**

Report of the Special rapporteur on extreme poverty and human rights**

Note by the Secretary-General

The Secretary-General has the honour to transmit to the General Assembly the report of the Special Rapporteur on extreme poverty and human rights, Philip Alston, submitted in accordance with Human Rights Council resolution 35/19.

Summary

The digital welfare state is either already a reality or is emerging in many countries across the globe. In these states, systems of social protection and assistance are increasingly driven by digital data and technologies that are used to automate, predict, identify, surveil, detect, target and punish. This report acknowledges the irresistible attractions for governments to move in this direction, but warns that there is a grave risk of stumbling zombie-like into a digital welfare dystopia. It argues that Big Tech operates in an almost human rights free-zone, and that this is especially problematic when the private sector is taking a leading role in designing, constructing, and even operating significant parts of the digital welfare state. The report recommends that instead of obsessing about fraud, cost savings, sanctions, and market-driven definitions of efficiency, the starting point should be on how welfare budgets could be transformed through technology to ensure a higher standard of living for the vulnerable and disadvantaged.

* A/74/50.

** The present report was submitted after the deadline in order to reflect the most recent developments.

Contents

	<i>Page</i>
I. Introduction.....	3
II. Uses of digital technologies in the welfare state.....	5
A. Identity verification	5
B. Eligibility assessment	7
C. Welfare benefit calculation and payments	8
D. Fraud prevention and detection	8
E. Risk scoring and need classification	9
F. Communication between welfare authorities and beneficiaries.....	9
III. Making digital technologies work for social protection	10
A. Taking human rights seriously and regulating accordingly.....	11
B. Ensuring legality and transparency.....	12
C. Promoting digital equality.....	13
D. Protecting economic and social rights in the digital welfare state	14
E. Protecting civil and political rights in the digital welfare state.....	15
F. Resisting the inevitability of a digital only future.....	17
G. The role of the private sector.....	18
H. Accountability mechanisms	18
IV. Conclusions.....	19

I. Introduction¹

1. The era of digital governance is upon us. In high and middle income countries, electronic voting, technology-driven surveillance and control including through facial recognition programs, algorithm-based predictive policing, the digitization of justice and immigration systems, online submission of tax returns and payments, and many other forms of electronic interactions between citizens and different levels of government are becoming the norm. And in lower income countries, national systems of biometric identification are laying the foundations for comparable developments, especially in systems to provide social protection, or ‘welfare’, to use a shorthand term.²

2. Invariably, improved welfare provision, along with enhanced security, is one of the principal goals invoked to justify the deep societal transformations and vast expenditures that are involved in moving the entire population of a country not just on to a national unique biometric identity card system but on to linked centralized systems providing a wide array of government services and the provision of goods ranging from food and education to health care and special services for the ageing or those with disabilities.

3. The result is the emergence of the ‘digital welfare state’ in many countries across the globe.³ In these states, systems of social protection and assistance are increasingly driven by digital data and technologies that are used to automate, predict, identify, surveil, detect, target and punish. The process is commonly referred to as ‘digital transformation’, but this somewhat neutral term should not be permitted to conceal the revolutionary, politically-driven, character of many such innovations. Commentators have predicted “a future in which government agencies could effectively make law by robot”,⁴ and it is clear that new forms of governance are emerging which rely significantly on the processing of vast quantities of digital data from all available sources, use predictive analytics to foresee risk, automate decision-making, and remove discretion from human decision-makers. In such a world, citizens become ever more visible to their governments, but not the other way around.⁵

4. Welfare is an attractive entry point not just because it takes up a major share of the national budget or affects such a large proportion of the population but because digitization can be presented as an essentially benign initiative. Thus, for example, the United Kingdom’s digital strategy proclaims that it will “transform the relationship between citizens and the state”, thus “putting more power in the hands of citizens and being more responsive to their needs.” In India, the core values of the Unique Identification Authority of India include: facilitating good governance, integrity, inclusive nation building, a collaborative approach, excellence in services, and transparency and openness.

5. In other words, the embrace of the digital welfare state is presented as an altruistic and noble enterprise designed to ensure that citizens benefit from new technologies, experience more efficient government, and enjoy higher levels of well-being. Often, however, the digitization of welfare systems has been accompanied by deep reductions in the overall welfare budget, a narrowing of the beneficiary pool, the elimination of some services, the introduction of demanding and intrusive forms of conditionality, the pursuit of behavioural modification goals, the imposition of stronger sanctions regimes, and a complete reversal of the traditional notion that the state should be accountable to the individual.

¹ This report has been prepared in close collaboration with Christiaan van Veen, Director of the Digital Welfare States and Human Rights Project, at New York University School of Law.

² While welfare is often used as a pejorative term, it is used in a positive sense in this report and is synonymous with the goal of social protection as reflected in the ILO’s Social Protection Floor initiative and comparable approaches. See generally David Garland, *The Welfare State: A Very Short Introduction* (2016).

³ Philip Alston and Christiaan van Veen, ‘How Britain’s welfare state has been taken over by shadowy tech consultants’, *The Guardian*, 27 June 2019.

⁴ Cary Coglianese and David Lehr, ‘Regulating by Robot: Administrative Decision Making in the Machine-Learning Era’, *Georgetown Law Journal* (Vol. 105, 2017), p. 1147.

⁵ Compare Foucault’s description of Panoptic systems where those put under surveillance are “seen, without ever seeing”. Michel Foucault, *Discipline and Punish: The Birth of the Prison* (1977), p. 202.

6. These other outcomes are promoted in the name of efficiency, targeting, incentivizing work, rooting out fraud, strengthening responsibility, encouraging individual autonomy, and responding to the imperatives of fiscal consolidation. Through the invocation of what are often ideologically-charged terms, neoliberal economic policies are seamlessly blended into what are presented as cutting edge welfare reforms, which in turn are often facilitated, justified, and shielded by new digital technologies. Although the latter are presented as being ‘scientific’ and neutral, they can reflect values and assumptions that are far removed from, and may be antithetical to, the principles of human rights. In addition, because of the relative deprivation and powerlessness of many welfare recipients, conditions, demands and forms of intrusiveness are imposed that would never have been accepted if they had instead been piloted in programs applicable to better-off members of the community.

7. Despite the enormous stakes involved not just for millions of individuals but for societies as a whole, these issues have, with a few notable exceptions,⁶ garnered remarkably little attention. The mainstream tech community has been guided by official pre-occupations with efficiency, budget-savings, and fraud detection. The welfare community has tended to see the technological dimensions as separate from the policy developments, rather than as being integrally linked. And those in the human rights community concerned with technology have understandably been focused instead on concerns such as the emergence of the surveillance state, the potentially fatal undermining of privacy, the highly discriminatory impact of many algorithms, and the consequences of the emerging regime of surveillance capitalism.

8. But the threat of a digital dystopia is especially significant in relation to the emerging digital welfare state. This report aims to redress the neglect of these issues to date by providing a systematic account of the ways in which digital technologies are used in the welfare state and of their implications for human rights. It concludes by calling for the regulation of digital technologies, including artificial intelligence, to ensure compliance with human rights, and for a rethinking of the positive ways in which the digital welfare state could be a force for the achievement of vastly improved systems of social protection.

9. The report builds in part on country reports by the Special Rapporteur on visits to the United States in 2017 and the United Kingdom in 2018 which drew attention to the increasing use of digital technologies in social protection systems. In preparing the report, the Special Rapporteur consulted with representatives of various digital rights groups, leading scholars, and other stakeholders, first in a meeting hosted by the Digital Freedom Fund in Berlin in February 2019, and then at another sponsored by the Center for Information Technology Policy at Princeton University in April 2019.⁷ In addition, a formal call for contributions resulted in some 60 submissions from 34 countries,⁸ including 22 governments, as well as international and national civil society organizations, National Human Rights Institutions, academics, and individuals. While it is impossible to do justice to these rich and detailed submissions in such a necessarily brief report, the Special Rapporteur has made them electronically available⁹ and will continue analyzing them in the context of ongoing work on the digital welfare state.¹⁰

⁶ For pioneering work on the impact of digital technologies on the American welfare state, especially on the poorest individuals in the system, see Virginia Eubanks, *Automating Inequality* (2018). See also Cathy O’Neil, *Weapons of Math Destruction* (2016) and Khiara Bridges, *The Poverty of Privacy Rights* (2017).

⁷ <https://www.princeton.edu/news/2019/04/18/panelists-tell-un-expert-artificial-intelligence-offers-promise-and-peril-social>.

⁸ From: Argentina, Australia, Austria, Azerbaijan, Brazil, Chile, Croatia, Egypt, El Salvador, Estonia, Germany, Greece, Guatemala, India, Italy, Ireland, Kazakhstan, Lebanon, Mexico, Nicaragua, Nigeria, Netherlands, New Zealand, Oman, Pakistan, Philippines, Poland, Qatar, Russian Federation, Senegal, South Africa, Switzerland, United Kingdom, and the United States.

⁹ <https://www.ohchr.org/EN/Issues/Poverty/Pages/SubmissionsGADigitalTechnology.aspx>.

¹⁰ <https://chrgj.org/people/christiaan-van-veen/>.

II. Uses of digital technologies in the welfare state

10. From the many submissions received, and on the basis of various case studies addressed in the literature, it is possible to distinguish various ways, and different stages in the welfare context, in which digital innovation has been most prominently used.

A. Identity verification

11. Establishing every person's legal identity, including through birth registration, by the year 2030 is the aim of Sustainable Development Goal (SDG) 16.9. A verifiable identity is essential for applying for benefits, establishing entitlement, receiving benefits, and appealing against denial. For the Government or other provider, it avoids duplication and fraud, it facilitates accurate targeting, and it enhances efficiency. Traditionally, paper and/or plastic documents have been used in forms such as birth certificates, identity cards and passports. These systems function reasonably well in most of the Global North, although 21 million adults in the United States do not have government-issued photo ID.¹¹ In the Global South, 502 million people in sub-Saharan Africa and 357 million in South Asia lack official identification.¹² In Liberia, for example, birth registration stands at only 5 per cent and national identity cards were not introduced until 2015.¹³

12. In response, the World Bank, regional development organizations and bilateral donors have launched new programs to promote access to identity documents. In particular, the World Bank's 'ID4D' (Identification for Development)¹⁴ campaign has focused heavily on promoting digital technologies as the key solution. This is explicitly stated in the 'Principles on Identification for Sustainable Development', which have been widely endorsed, including by MasterCard.¹⁵

13. The Principles acknowledge that there are both pros and cons involved. On the positive side, it is claimed that digital technology can "create huge savings for citizens, governments, and businesses by reducing transaction costs, increasing efficiency, and driving innovation in service delivery, particularly to the poorest and most disadvantaged groups in society".¹⁶ Digital identity systems can also "improve governance, boost financial inclusion, reduce gender inequalities by empowering women and girls, and increase access to health services and social safety nets for the poor".¹⁷

14. But in addition to this impressive and by now familiar sales pitch, the Principles, and similar documents,¹⁸ also recognize possible downsides ranging from political backlash to privacy and (cyber)security concerns. Solutions for dealing with those risks are often either technological or take the form of soft law norms. Thus a comparable United States Agency for International Development (USAID) document calls for "open source solutions" and developing good "practices for data privacy" to resolve the relevant problems. While the World Bank Principles refer to isolated human rights principles such as Article 7 of the

¹¹ <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/PrivacyInternational.pdf>

¹² USAID, 'Identity in a Digital Age' (2017), p. 8.

¹³ Bronwen Manby, *Citizenship in Africa* (2018), p. 3.

¹⁴ <https://id4d.worldbank.org/>

¹⁵ World Bank and Center for Global Development, 'Principles on Identification for Sustainable Development: Toward the Digital Age', February 2017, at <http://documents.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf>

¹⁶ World Bank and Center for Global Development, 'Principles on Identification for Sustainable Development: Toward the Digital Age', February 2017, p. 5, available from: <http://documents.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf>;

¹⁷ Id.

¹⁸ USAID, 'Identity in a Digital Age' (2017); McKinsey, 'Digital Identification: A Key to Inclusive Growth', January 2019, at <https://www.mckinsey.com/~media/mckinsey/featured%20insights/innovation/the%20value%20of%20digital%20id%20for%20the%20global%20economy%20and%20society/digital-id-a-key-to-inclusive-growth-january%202019.ashx>

Convention on the Rights of the Child, they rely primarily on the need to create an interoperable system using open standards, and protecting ‘privacy through system design’.

15. The world’s largest biometric identification system is Aadhaar in India, which is a 12-digit unique identifying number issued to Indian residents. It contains both demographic and biometric information, including an iris scan, a photograph and fingerprints. It is used to verify the identity of recipients of benefits and subsidies and is now mandatory to access those social rights.¹⁹ It was first introduced in 2009 and now covers more than 1.2 billion people,²⁰ and has been enthusiastically endorsed by the international development community.²¹ The World Bank has praised it for “overcoming complex information problems, [thereby helping] willing governments to promote the inclusion of disadvantaged groups”,²² and has enthusiastically encouraged other governments to learn from the experience,²³ and over 20 countries are reported to have expressed an interest in emulating Aadhaar.²⁴

16. It nevertheless remains controversial domestically. Critics have reportedly been harassed and surveilled for their opposition,²⁵ and the scheme has been criticized for unnecessarily collecting biometric information, for severe shortcomings in legislative oversight, function creep, facilitating surveillance and other intrusions on the right to privacy, exacerbating cybersecurity issues, and creating barriers to accessing a range of social rights.²⁶

17. In 2018 India’s Supreme Court, in a 1448-page landmark ruling, upheld Aadhaar’s constitutionality, albeit with some caveats. The court appeared to view the use of biometric identification technology in the context of providing welfare benefits as being legitimate, proportional and even inevitable. In a welfare state, Aadhaar’s aim of ensuring that benefits reach the intended beneficiary was “naturally a legitimate State aim”.²⁷ In balancing the rights to social security and privacy, the court held that registering biometric data represented a ‘minimal’ inroad into privacy rights,²⁸ and went so far as to characterize Aadhaar as “a vital tool of ensuring good governance in a social welfare state”.²⁹ But the Supreme Court’s ruling has apparently not put an end to the controversy surrounding the scheme.³⁰

18. In 2019 Kenya required all of its citizens, including those living abroad, and all foreign nationals and refugees in the country, above the age of 6, to obtain a national ID in order to access government services, including welfare benefits.³¹ This involved providing biometric data including fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves and DNA in digital form. In response to a case claiming that this Huduma Namba program violated the rights to privacy, equality, non-discrimination and public participation, the High Court issued an interim order allowing the registration process to continue, but on a voluntary basis and on the basis that the disbursement of government services and benefits could not be made conditional on participation. Subsequently, registration has proceeded

¹⁹ See, e.g., Centre for Communication Governance at National Law University Delhi, at <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/NationalLawUniversityDelhi.pdf>.

²⁰ <https://economictimes.indiatimes.com/news/politics-and-nation/national-population-register-to-include-aadhaar-details/articleshow/70528850.cms?from=mdr>.

²¹ Jeanette Rodrigues, ‘India ID Program Wins World Bank Praise Despite ‘Big Brother’ Fears’, 15 March 2017, available from: <https://www.bloomberg.com/news/articles/2017-03-15/india-id-program-wins-world-bank-praise-amid-big-brother-fears>.

²² World Bank, *World Development Report 2016*, p. 2.

²³ <https://www.livemint.com/Politics/UEQ9o8Eo8RiaAaNNMyLbEK/Aadhaar-goes-global-finds-takers-in-Russia-and-Africa.html>.

²⁴ <https://factordaily.com/aadhaar-india-stack-export/>.

²⁵ <https://www.reuters.com/article/us-india-aadhaar-breach/critics-of-indias-id-card-project-say-they-have-been-harassed-put-under-surveillance-idUSKBN1FX0H0>

²⁶ Submission to the Special Rapporteur by the National Law University, Delhi.

²⁷ Supreme Court of India, Writ Petition (Civil) No. 494 of 2012, p. 341.

²⁸ *Id.*, p. 377.

²⁹ *Id.*, p. 553.

³⁰ <https://www.nytimes.com/2018/09/26/technology/india-id-aadhaar-supreme-court.html>.

³¹ Amnesty International, at <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/AmnestyInternational.pdf>.

apace, some two-thirds of the population has been registered,³² and the Government is reportedly threatening to exclude unregistered individuals from access to benefits or the right to vote.³³

19. In South Africa, the South African Social Security Agency (SASSA), distributes non-contributory and means-tested social grants to around one-third of the population, including for example grants for child support, for pensioners, and for persons with disabilities.³⁴ In 2012, SASSA contracted with the company Cash Paymaster Services (CPS), a subsidiary of Net1, to deliver the grants.³⁵ CPS registered beneficiaries by collecting their biometric information (finger prints and, originally, voice recordings) and beneficiaries were issued MasterCard debit cards with biometric functionality and a linked bank account by Net1 and Grindrod Bank in association with SASSA.³⁶ After much controversy surrounding the tender to CPS, the fees charged by CPS, deductions made to social grants on these accounts as well as privacy concerns surrounding the processing of card holder data, SASSA changed providers in 2018 by entering into a partnership with the South African Post Office (SAPO). SASSA and SAPO will provide new biometric cards. The change from CPS to SAPO has been complex and has led to questions about effective access to social grants by beneficiaries in South Africa.³⁷

20. Many other examples could be given of countries using or exploring digital identity systems, including Argentina,³⁸ Bangladesh,³⁹ Chile,⁴⁰ Ireland, Jamaica,⁴¹ Malaysia,⁴² the Philippines,⁴³ and the United States.⁴⁴

B. Eligibility assessment

21. Automated programs are increasingly used to assess eligibility in many countries. An especially instructive case was the automation of eligibility decisions in Ontario in 2014 through the Social Assistance Management System (SAMS) which relied on Cúram, a customizable off-the-shelf IBM software package, also used in welfare programs in Canada, the United States, Germany, Australia and New Zealand.⁴⁵

22. In 2015 the Ontario Auditor-General reported on 1,132 cases of errors with eligibility determinations and payment amounts under SAMS involving about \$140 million. The total expenditure on SAMS by late 2015 was \$290 million.⁴⁶ The new system reportedly led caseworkers to resort to subterfuges to ensure that beneficiaries were fairly treated, made decisions very difficult to understand, and created significant additional work for staff.⁴⁷

³² Id.

³³ <https://www.standardmedia.co.ke/article/2001334286/you-ll-miss-vital-services-without-huduma-namba>.

³⁴ <https://www.dfa.co.za/news/budget2019-social-grants-to-increase-19404725>.

³⁵ Black Sash, at <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/BlackSash.pdf>.

³⁶ <https://newsroom.mastercard.com/press-releases/more-than-2-5-million-mastercard-debit-cards-issued-to-social-welfare-beneficiaries-in-south-africa/>.

³⁷ <https://citizen.co.za/business/1944057/post-office-set-to-take-over-cash-payments-from-cps/>.

³⁸ Submission to the Special Rapporteur by the Government of Argentina.

³⁹ <https://privacyinternational.org/examples/2878/bangladesh-biometrics-needed-access-welfare-payment>.

⁴⁰ In Chile, facial recognition technology is used to deliver school meals: See <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/PrivacyInternational.pdf>.

⁴¹ <https://opm.gov.jm/portfolios/national-identification-system/>.

⁴² <https://www.opengovasia.com/malaysias-digital-id-project-to-be-finalised-by-2019/>.

⁴³ <https://psa.gov.ph/philsys>.

⁴⁴ See for example the use of digital technologies in the CalWORKs program in California, the United States, at <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/HumanRightsWatch.pdf>.

⁴⁵ Submission to the Special Rapporteur by Human Rights Watch, available from: <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/HumanRightsWatch.pdf>.
⁴⁶ *2015 Annual Report of the Office of the Auditor General of Ontario*, p. 475.

⁴⁷ Jennifer Raso, 'Displacement as Regulation: New Regulatory Technologies and Front Line Decision Making in Ontario Works', *Canadian Journal of Law and Society*, Vol. 32, (2017) 75.

C. Welfare benefit calculation and payments

23. The calculation and payment of benefits is increasingly done through digital technologies without the involvement of caseworkers and other human decision-makers. While such systems offer many potential advantages, the Special Rapporteur also received information about prominent examples of system errors or failures that generated major problems for large numbers of beneficiaries. These included the ‘Robodebt’ fiasco in Australia,⁴⁸ the Real Time Information system in the United Kingdom,⁴⁹ and the SAMS system in Canada.

24. Electronic payment cards or debit cards are also increasingly being issued to welfare recipients. Information provided to the Special Rapporteur in relation to such programs in New Zealand, Australia and South Africa reveal very similar problems. First, beneficiaries often face difficulties accessing and fully utilizing their right to social security.⁵⁰ Second, when such cards are clearly recognizable as welfare-related, users have expressed feelings of disempowerment, embarrassment and shame,⁵¹ a problem exacerbated when the users come from communities long accustomed to exclusion.⁵² Third, electronic cards enable monitoring and surveillance of behavioral data by welfare authorities and private actors, thus raising important human rights concerns.⁵³

25. Fourth, the outsourcing of the issuance and administration of electronic cards to private companies has led to problems such as users being encouraged to pay for commercial financial products and the imposition of user fees.⁵⁴ More generally the ethos surrounding such cards has often reflected stereotypes such as the financial untrustworthiness and irrationality of those living in poverty.

D. Fraud prevention and detection

26. Fraud and error in welfare systems can potentially involve very large sums of money and have long been a major concern for governments. It is thus unsurprising that many of the digital welfare systems that have been introduced have been designed with a particular emphasis on the capacity to match data from different sources in order to expose deception and irregularities on the part of welfare applicants. Nevertheless, evidence from country missions undertaken by the Special Rapporteur,⁵⁵ along with other cases examined,⁵⁶ suggests that the magnitude of these problems is frequently overstated and that there is sometimes a wholly disproportionate focus on this particular dimension of the complex welfare equation. Images of supposedly wholly undeserving individuals receiving large government welfare payments, such as Ronald Reagan’s ‘welfare queen’ trope, have long been used by conservative politicians to discredit the very concept of social protection. The risk is that the digital welfare state provides endless possibilities for taking surveillance and intrusion to new and deeply problematic heights.

⁴⁸ Terry Carney, ‘The New Digital Future for Welfare: Debts Without Legal Proofs or Moral Authority?’, *UNSW Law Journal Forum* (March, 2018) p. 1; Report by the Acting Commonwealth Ombudsman, Richard Glenn, ‘Centrelink’s automated debt raising and recovery system’, April 2017, p. 7-8; Submission to the Special Rapporteur by Monash University.

⁴⁹ Statement on Visit to the United Kingdom, 16 November 2018, at: <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23881&LangID=E>.

⁵⁰ <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/GriffithUniversity.docx>.

⁵¹ <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/NicoleNaujokas.docx>.

⁵² <https://www.theguardian.com/australia-news/2017/jan/09/ration-days-again-cashless-welfare-card-ignites-shame>.

⁵³ <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/UniversityAuckland.docx>.

⁵⁴ <http://theconversation.com/the-real-risks-behind-south-africas-social-grant-payment-crisis-73224>

⁵⁵ Statement on Visit to the United Kingdom, by Professor Philip Alston, United Nations Special Rapporteur on extreme poverty and human rights, 16 November 2018, available from: <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23881&LangID=E>.

⁵⁶ See the SyRI case from the Netherlands, n86 below.

E. Risk scoring and need classification

27. Risk calculation is inevitably at the heart of the design of welfare systems and digital technologies can achieve very high levels of sophistication in this regard. In addition to fraud detection and prevention, child protection has been a major focus in this area, as illustrated by examples from countries as diverse as the United States,⁵⁷ New Zealand,⁵⁸ the United Kingdom,⁵⁹ and Denmark.⁶⁰ Governments have also applied these techniques to determine whether unemployment assistance will be provided and at what level. A prominent such scheme in Poland was held unconstitutional,⁶¹ but an algorithm-based system in Austria continues to categorize unemployed jobseekers to determine the support they will receive from government jobcenters.⁶²

28. Many other areas of the welfare state will also be affected by new technologies used to score risks and classify needs.⁶³ While such approaches offer many advantages, it is also important to take account of the problems that can arise. First there are many issues raised by determining an individual's rights on the basis of predictions derived from the behavior of a general population group.⁶⁴ Second, the functioning of the technologies and how they arrive at a certain score or classification is often secret, thus making it difficult to hold governments and private actors to account for potential rights violations.⁶⁵ Third, risk-scoring and need categorization can reinforce or exacerbate existing inequalities and discrimination.⁶⁶

F. Communication between welfare authorities and beneficiaries

29. Communications that previously took place in person, by phone or by letter are increasingly being replaced by online applications and interactions. Various submissions to the Special Rapporteur cited problems with the Universal Credit system in the United Kingdom, including difficulties linked to a lack of internet access and/or digital skills,⁶⁷ and

⁵⁷ Virginia Eubanks, *Automating Inequality* (2018); Alexandra Chouldechova et. al., 'A case study of algorithm-assisted decision making in child maltreatment hotline screening decisions', *Proceedings of Machine Learning Research* 81:1–15, 2018; <https://www.nytimes.com/2018/01/02/magazine/can-an-algorithm-tell-when-kids-are-in-danger.html>.

⁵⁸ Philip Gillingham, 'Predictive Risk Modelling to Prevent Child Maltreatment: Insights and Implications from Aotearoa/New Zealand', *Journal of Public Child Welfare* (Vol. 11, 2017), p. 150.

⁵⁹ <https://www.theguardian.com/society/2018/sep/16/councils-use-377000-peoples-data-in-efforts-to-predict-child-abuse>; <https://www.communitycare.co.uk/2019/06/14/county-becomes-latest-authority-trial-predictive-algorithms-childrens-social-work/>.

⁶⁰ <https://foreignpolicy.com/2018/12/25/the-welfare-state-is-committing-suicide-by-artificial-intelligence/>.

⁶¹ Polish Supreme Court, case K 53/16, 6 June 2018, <http://trybunal.gov.pl/postepowanie-i-orzeczenia/komunikaty-prasowe/komunikaty-po/art/10168-zarzadzanie-pomoca-kierowana-do-osob-bezrobotnych>.

⁶² EpicenterWorks, at <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/EpicenterWorks.pdf>

⁶³ See, for example, Data Justice Lab, 'Data Scores as Governance: Investigating uses of citizen scoring in public services', December 2018.

⁶⁴ University of Queensland, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/University_of_Queensland.pdf; and Data Justice Lab, at

<https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/UniversityCardiff.pdf> ("Household-level and individual-level data relies on a fundamental personalization of risk, attaching risk factors to individual characteristics and behaviour that can lead to individualized responses to social ills being privileged over collective and structural responses, such as issues of inequality, poverty or racism.").

⁶⁵ London School of Economics and Political Science, at <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/LSE.pdf>.

⁶⁶ "But human bias is built in to the predictive risk model." <https://www.wired.com/story/excerpt-from-automating-inequality/>.

⁶⁷ Scottish Council for Voluntary Organisations, at <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/ScottishCouncilVoluntaryOrganisations.pdf>; and Citizens Advice Scotland, at

the extent to which online portals can create confusion and obfuscate legal decisions, thereby undermining the right of claimants to understand and appeal decisions affecting their social rights.⁶⁸ Similar issues were also raised in relation to other countries including Australia,⁶⁹ and Greece.⁷⁰

30. Another problem is the likelihood that once the entire process of applying and maintaining benefits is moved online, the situation invites further digital innovation. In 2018 Sweden was forced to reverse a complex digital system used by the Employment Service to communicate with jobseekers because of problems that led to as many as 15% of the system's decisions probably being incorrect.⁷¹

31. Australia's Targeted Compliance Framework (TCF) requires job seekers to interact with a digital dashboard to report mandatory activities and to check their compliance status. Failure to meet a 'mutual obligation' can automatically, without the involvement of a human decision-maker, lead to suspension of payments or the imposition of financial penalties. Submissions have highlighted problems due to a lack of internet access and digital literacy, to the rigidity of an automated system which fails to take real-life situations into account.⁷²

III. Making digital technologies work for social protection

32. Digital technologies, including artificial intelligence, have huge potential to promote the many benefits that are consistently cited by their proponents. They are already doing so for those who are economically secure and can afford to pay for the new services. They could also make an immense positive difference in improving the well-being of the less well-off members of society, but this will require deep changes in existing policies. The leading role in any such effort will have to be played by governments through appropriate fiscal policies and incentives, regulatory initiatives, and a genuine commitment to designing the digital welfare state not as a Trojan Horse for neoliberal hostility towards welfare and regulation but as a way to ensure a decent standard of living for everyone in society.

33. This report has sought to highlight problems that are specific to the ways in which the digital welfare state has been envisioned and implemented. But many of the changes required to avoid a digital dystopia will need to range more broadly. In addressing the General Assembly on 24 September 2019 the Prime Minister of the United Kingdom warned of the dangers of the digital age, singling out: (i) the risk of 'round-the-clock surveillance'; (ii) the perils of algorithmic decision-making; (iii) the difficulty of appealing against computer-generated determinations; and (iv) the inability to plead extenuating circumstances when the decision-maker is an algorithm. He concluded rather ominously by suggesting that "[d]igital authoritarianism is ... an emerging reality."⁷³

34. His comments resonate strongly in the context of the digital welfare state, including in relation to the United Kingdom's Universal Credit system. There is no magic recipe for

https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/ChildPovertyActionsGroup_1.pdf.

⁶⁸ Child Poverty Action Group, 'Computer Says No!', May 2019, available from: https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/ChildPovertyActionsGroup_2.pdf.

⁶⁹ Senate Community Affairs References Committee, Parliament of Australia, *Design, scope, cost-benefit analysis, contracts awarded and implementation associated with the Better Management of the Social Welfare System Initiative* (June, 2017), p. 60.

⁷⁰ Submission to the Special Rapporteur by the Government of Greece.

⁷¹ AlgorithmWatch, 'Sweden: Rogue algorithm stops welfare payments for up to 70,000 unemployed', 19 February 2019.

⁷² Human Rights Law Centre, at <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/HumanRightsLawCentre.pdf>; and <https://www.nssrn.org.au/social-security-rights-review/the-targeted-compliance-framework-implications-for-job-seekers/>.

⁷³ <https://www.gov.uk/government/speeches/pm-speech-to-the-un-general-assembly-24-september-2019>.

avoiding the pitfalls of which he warned, but the following steps could help to make the digital welfare state a force for enhancing rather than undermining human rights.

A. Taking human rights seriously and regulating accordingly

35. The United Kingdom Prime Minister concluded his speech by warning that “[u]nless we ensure that new technology reflects” human rights, the Universal Declaration of Human Rights “will mean nothing”⁷⁴ But the reality is that governments have certainly not regulated the tech industry as if human rights were at stake, and the technology sector remains virtually a human rights-free zone. The Big Tech companies and their governmental supporters have worked hard to keep it that way. Their approach can be summed up for present purposes in four propositions.

36. The first is that the ability to innovate requires freedom, especially from regulation. The Facebook founder’s early call for the industry to “move fast and break things” epitomizes the importance attached to minimizing legal and governmental constraints. Yet this argument leads inexorably to a handful of powerful executives replacing governments and legislators in determining the directions in which societies will move and the values and assumptions which will drive those developments. The accumulation of vast amounts of capital in the hands of very small elites and the rapid growth in extreme inequality have gone hand in hand with the ascendancy of this approach so far.⁷⁵

37. The second proposition is that there are no universal values. In a recent book, the President of Microsoft asked rhetorically: “How can the world converge on a singular approach to ethics for computers when it cannot agree on philosophical issues for people?”⁷⁶ Even non-discrimination standards are sometimes presented as being too vague and contested to be useful in regulating AI.⁷⁷ But these arguments are self-serving and ill-informed. Governments worldwide have accepted universal human rights standards, including in the form of binding legal obligations. And over the past half century or more, these standards have been exhaustively developed and applied by courts, and a wide range of expert and community-based bodies. There remains plenty of room for philosophical disagreements, but there is no absence of agreement on core human values.

38. The third proposition is that governments are inherently slow and clumsy, and tend to respond to yesterday’s challenges rather than tomorrow’s. As the Republican minority leader of the United States House of Representatives recently argued, “the bureaucratic leviathan [does not have] what it takes to develop or enforce nimble responses to rapid change in the technology industry.”⁷⁸ But while such claims might also be put forward by the proponents of unfettered discretion for the finance, aviation, defence, pharmaceutical, and other industries, it is solely in relation to Big Tech that governments have been prepared to abandon their regulatory responsibilities and acquiesce in a self-regulatory approach to such an extreme degree. There is no justification for such exceptionalism and no empirical evidence to support the claim that there is a fundamental incompatibility between innovation and regulation.

39. And the fourth proposition is that public accountability is unnecessary because the free market is the best regulator.⁷⁹ Leaving aside the powerful arguments that Big Tech is

⁷⁴ Id.

⁷⁵ See generally Shoshana Zuboff, *The Age of Surveillance Capitalism* (2019); and Emmanuel Saez and Gabriel Zucman, *The Triumph of Injustice: How the Rich Dodge Taxes and How to Make Them Pay* (2019).

⁷⁶ Brad Smith and Carol Ann Browne, *Tools and Weapons: The Promise and the Peril of the Digital Age* (2019), p. 207.

⁷⁷ *Public Scrutiny of Automated Decisions: Early Lessons and Emerging Methods, An Upturn and Omidyar Network Report* (2018), p. 25, and n. 115 at https://www.omidyar.com/sites/default/files/file_archive/Public%20Scrutiny%20of%20Automated%20Decisions.pdf.

⁷⁸ Kevin McCarthy, ‘Don’t Count on Government to Protect Your Privacy’, *New York Times*, 14 June 2019.

⁷⁹ See generally Julie Cohen, ‘Law for the Platform Economy’, *51 U.C. Davis L. Rev.* 133 (2017).

deeply anti-competitive and thus immune to many currents of the free market, the great scandals of recent years that have led to the so-called ‘techlash’ provide compelling evidence that public accountability is indispensable.

40. In response to growing calls for effective governmental regulation, the industry has gone into high gear in producing, influencing and embracing ‘codes of ethics’ and other non-binding standards purporting to ‘regulate’ digital technologies and their developers.⁸⁰ Most, but by no means all, of these codes contain a reference to human rights, but the substance of human rights law is invariably lacking. Instead the token reference to human rights serves only to enhance claims to legitimacy and universality. Meanwhile, the relevant discussions of ethics are based on almost entirely open-ended notions that are not necessarily grounded in legal or even philosophical arguments, and can be shaped to suit the needs of the industry. As a result, there are serious problems of conceptual incoherence, conflicts among norms are rarely acknowledged, meaningful input is rarely sought from stakeholders, and accountability mechanisms are absent.⁸¹ Even industry-employed ethicists acknowledge that “[i]f ethics is simply absorbed within the logics of market fundamentalism, meritocracy, and technological solutionism, it is unlikely that the tech sector will be able to offer a meaningful response to the desire for a more just and values-driven tech ecosystem.”⁸² Against this background, it is unsurprising that there are few public or scholarly discussions of the *human rights* implications of digital welfare states.

41. The human rights community has thus far done a very poor job of persuading industry, government, or seemingly society at large, of the fact that a technologically-driven future will be disastrous if it is not guided by respect for human rights that is in turn grounded in law.

B. Ensuring legality and transparency

42. One of the most surprising characteristics of too many important digital welfare state initiatives is a lack of attention to the importance of ensuring legality. Many examples have been drawn to the Special Rapporteur’s attention, including: the Australian Government’s online compliance intervention system which used automated data-matching as the basis to send out vast numbers of debt notices with very high error rates (known as Robodebt);⁸³ allegedly unlawful information provided to claimants via the online Universal Credit portal in the United Kingdom;⁸⁴ the contested legality of the Irish Public Services Card for some of the purposes for which it has been used;⁸⁵ the SyRI (System Risk Indication) system in the

⁸⁰ These include industry standards, civil society initiatives and public frameworks. To give a few examples: IBM, ‘Everyday Ethics for Artificial Intelligence’ (September 2018); Google, ‘AI Principles’ (2019); Microsoft, *The Future Computed* (2018); IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems; SIIA, ‘Ethical Principles for Artificial Intelligence and Data Analytics’ (2017); Asilomar AI Principles (2017); Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, ‘Ethics Guidelines for Trustworthy AI’ (April 2019).

⁸¹ Karen Yeung, Andrew Howes, and Ganna Pogrebnia, ‘AI Governance by Human Rights-Centred Design, Deliberation and Oversight: An End to Ethics Washing’, forthcoming in M Dubber and F Pasquale (eds.), *The Oxford Handbook of AI Ethics* (2019), at <https://ssrn.com/abstract=3435011>, p. 22.

⁸² Jacob Metcalf, Emanuel Moss, and danah boyd [sic], ‘Owning Ethics: Corporate Logics, Silicon Valley, and the Institutionalization of Ethics’, 82 *Social Research* (2019) 449, at 473.

⁸³ Terry Carney, ‘The New Digital Future for Welfare: Debts Without Legal Proofs or Moral Authority?’, *UNSW Law Journal Forum* (March 2018).

⁸⁴ https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/ChildPovertyActionsGroup_1.pdf.

⁸⁵ Final Investigation Report: ‘An investigation by the Data Protection Commission in respect of the processing of personal data by the Department of Employment Affairs and Social Protection in relation to the Public Services Card (“PSC”) examining compliance with the obligations in relation to Legal Basis and Transparency’ (2019), at <https://www.welfare.ie/en/pdf/pr170919.pdf>.

Netherlands which initially lacked a legal basis and remains subject to court challenge;⁸⁶ and the Aadhaar system in India which was originally implemented without a legal framework.⁸⁷

43. While the lack of a legal basis is deeply problematic per se, this gap also means that opportunities for legislative debate and for public inputs into shaping the relevant systems is also lacking. This has major potentially negative implications for transparency, design, legitimacy, and the likelihood of acceptance.

C. Promoting digital equality

44. Egalitarianism is a consistent theme of the technology industry, as exemplified by Facebook's aim "to give people the power to build community and bring the world closer together".⁸⁸ But at the macro level Big Tech has been a driver of growing inequality⁸⁹ and has facilitated the creation of a 'vast digital underclass'.⁹⁰

45. For its part, the digital welfare state sometimes gives beneficiaries the option to go digital or continue using more traditional techniques. But in reality, policies such as 'digital by default' or 'digital by choice' are usually transformed into 'digital only' in practice. This in turn exacerbates or creates major disparities among different groups. A lack of digital literacy leads to an inability to use basic digital tools at all, let alone effectively and efficiently. Limited access, or no access to the internet, poses huge problems for a great many people. Additional barriers arise for individuals who have to pay high prices to obtain internet access, to travel long distances or absent themselves from work to do so, visit public facilities such as libraries in order to get access, or obtain assistance from staff or friends to navigate the systems. And while the well-off might have instant access to up-to-date, and easy to use computers and other hardware, as well as fast and efficient broadband speeds, the least well off are far more likely to be severely disadvantaged by out of date equipment and time-consuming and unreliable digital connections.

46. Submissions to the Special Rapporteur from a wide range of countries emphasized the salience of these different problems. Both in the Global North and the Global South, many individuals, and especially those living in poverty, do not have a reliable internet connection at home,⁹¹ cannot afford such a connection,⁹² are not digitally skilled or confident,⁹³ or are otherwise inhibited in communicating with authorities online. The various submissions emphasize how these problems impede the ability of would-be claimants to realize their human rights.

⁸⁶ Brief by the United Nations Special Rapporteur on extreme poverty and human rights as Amicus Curiae in the case of NJCM c.s./De Staat der Nederlanden (SyRI) before the District Court of The Hague (case number: C/09/550982/ HA ZA 18/388) (September 2019), at <https://www.ohchr.org/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf>.

⁸⁷ Submission to the Special Rapporteur by National Law University Delhi, available from: <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/NationalLawUniversityDelhi.pdf>.

⁸⁸ Kevin Munger, 'The Rise and Fall of the Palo Alto Consensus', *New York Times*, 10 June 2019.

⁸⁹ Isobel Asher Hamilton, 'A definitive list of the 13 richest tech billionaires in the world', *Business Insider*, 9 March 2019, available from: <https://www.businessinsider.nl/net-worth-13-richest-tech-billionaires-in-the-world-2019-3?international=true&r=US>.

⁹⁰ Farhad Manjoo, 'The Tech Industry is Building a Vast Digital Underclass', *The New York Times*, 24 July 2019.

⁹¹ <https://www.wired.com/story/global-internet-access-dire-reports/>; <https://data.oecd.org/ict/internet-access.htm>; <https://www.oecd.org/internet/oecd-toolkit-aims-to-spur-high-speed-internet-use-in-latin-america-and-the-caribbean.htm>.

⁹² https://a4ai.org/affordability-report/report/2018/#2018:_where_are_we_on_the_road_to_affordable_universal_internet_access?; <https://webfoundation.org/2019/03/new-mobile-broadband-pricing-data-reveals-stalling-progress-on-affordability/>; In the United States, 27% of the population does not use high-speed broadband internet at home, and that figure is as high as 44% for people with an income below \$30,000: <https://www.pewinternet.org/fact-sheet/internet-broadband/>.

⁹³ European Commission, 'Human Capital: Digital Inclusion and Skills' (2019).

47. The United Kingdom provides an example of a wealthy country in which, even in 2019, 11.9 million people (22% of the population) do not have the ‘essential digital skills’ needed for day-to-day life. An additional 19% cannot perform fundamental tasks such as turning on a device or opening an app. In addition, 4.1 million adults (8%) are offline because of fears that the internet is an insecure environment, and proportionately almost half of those are from a low income household and almost half are under sixty years of age.⁹⁴

48. These problems are compounded by the fact that when digital technologies are introduced in welfare states, their distributive impact is often not a significant focus of governments.⁹⁵ In addition, vulnerable individuals are not commonly involved in the development of IT systems and the IT professionals are often ill-equipped to anticipate the sort of problems that are likely to arise.⁹⁶ Programs often assume, without justification, that individuals will have ready access to official documents and be able to upload them, that they will have a credit history or broader digital financial footprint, or even that their fingerprints will be readable, which is often not the case for those whose working lives have involved unremitting manual labour.

49. In terms of digital welfare policy, several conclusions emerge. First, there should always be a genuine non-digital option available.⁹⁷ Second, programs that aim to digitize welfare arrangements should be accompanied by programs designed to promote and teach the needed digital skills and to ensure reasonable access to the necessary equipment as well as effective online access. Third, in order to reduce the harm caused by incorrect assumptions and mistaken design choices, digital welfare systems should be co-designed by their intended users and evaluated in a participatory manner.

D. Protecting economic and social rights in the digital welfare state

50. The processes of digitization and the increasing role played by automated decision-making through the use of algorithms and artificial intelligence have, in at least some respects, facilitated a move towards a bureaucratic process and away from one premised on the right to social security or the right to social protection. Rather than the ideal of the State being accountable to the citizen to ensure that the latter is able to enjoy an adequate standard of living, the burden of accountability has in many ways been reversed. To a greater degree than has often been the case in the past, today’s digital welfare state is often underpinned by the starting assumption that the individual is not a rights-holder but rather an applicant. In that capacity, a person must convince the decision-maker that they are ‘deserving’, that they satisfy the eligibility criteria, that they have fulfilled the often onerous obligations prescribed, and that they have no other means of subsistence. And much of this must be done electronically, regardless of the applicant’s skills in that domain.

51. The right to social security⁹⁸ encompasses the right “to access and maintain benefits, whether in cash or in kind, without discrimination”.⁹⁹ The imposition of technological

⁹⁴ ‘The Digitally Disadvantaged’, in *UK Consumer Digital Index 2019 – Key Findings* (Lloyds Bank 2019).

⁹⁵ <https://www.nytimes.com/2019/04/25/opinion/privacy-poverty.html>.

⁹⁶ Submission to the Special Rapporteur by ICTU, available from: <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/ITCU.pdf>.

⁹⁷ Association for Progressive Communications, *Derechos Digitales and Media Matters for Democracy*, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/APC_DerechosDigitalesMedia.pdf; Citizens Advice Scotland, at <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/CitizensAdviceScotland.pdf>; National Social Security Rights Network, at <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/NationalSocialSecurityRightsNetwork.pdf>.

⁹⁸ Article 9 of the International Covenant on Economic, Social and Cultural Rights (ICESCR).

⁹⁹ Committee on Economic, Social and Cultural Rights, *The Right to Social Security*, General Comment No. 19 (2007), para. 2.

requirements can make it impossible or very difficult for individuals to effectively access that right, thus making it effectively unaffordable.¹⁰⁰

52. The right to social protection is integrally linked to what the Human Rights Committee refers to as the right to life with dignity, which must be protected, where necessary, through “measures designed to ensure access without delay by individuals to essential goods and services such as food, water, shelter, health-care, electricity and sanitation, and other measures designed to promote and facilitate adequate general conditions ...”.¹⁰¹ Various other rights are also implicated, including the right to an adequate standard of living, the right to mental health, and the right to be treated with dignity.

53. While social protection in general should be designed to protect these rights, the dignity dimension is at particular risk in the context of the digital welfare state. The potential risks arise in various contexts. First, the process for determining eligibility can easily be transformed into an electronic question and answer process that almost inevitably puts already vulnerable individuals at even greater disadvantage. Second, the way in which determinations are framed and communicated can be dehumanized and allow no room for meaningful questioning or clarification.

54. Third, the digital welfare state often seems to involve various forms of rigidity and the robotic application of rules. As a result, extenuating circumstances such as being late for an appointment because of urgent caring obligations, or being unable to understand a written communication whether because of a disability or a personal crisis, are often not taken into account in a predominantly digital context. Fourth, digital systems are often not designed to respond rapidly either to serious emergencies or to the daily challenges experienced by an older person whose entitlement has suddenly and inexplicably been electronically reduced or cancelled, or by a single parent unable to take a child to a local day care because the digital ID card will not function.

55. Fifth, the ways in which services are provided can easily have degrading connotations, such as unnecessarily exposing to a broader audience the fact that a person is reliant on benefits, or requiring extended waiting periods, or the navigation of lengthy queues. Sixth, the introduction of various new technologies that eliminate the human provider can enhance efficiency and provide other advantages, but might not necessarily be satisfactory for individuals who are in situations of particular vulnerability. New technologies often operate on the law of averages, in the interests of majorities, and on the basis of predicted outcomes or likelihoods.

56. Sixth, digital services risk eliminating, almost entirely, much of the human interaction and compassion that are likely to be indispensable components in providing at least some welfare recipients with the care and assistance they need. The assumption that there is always a technological fix for any problem is highly likely to be misplaced in various aspects of a humane and effective system of social protection.

E. Protecting civil and political rights in the digital welfare state

57. That the poor suffer from more intense levels of scrutiny, monitoring, surveillance, is hardly an original observation. In the 1960s, Charles Reich wrote that welfare recipients in the United States “have been subjected to many forms of procedure and control not imposed on other citizens. ... [They] are all too easily regulated.”¹⁰² In 1975, Michel Foucault wrote about the ‘coercive technologies of behavior’ used in modern society to ‘discipline and punish’ the poorer classes.¹⁰³

58. By way of explaining why these lessons have not been learned in the digital welfare state, Shoshana Zuboff writes that the system of ‘surveillance capitalism’ that prevails today

¹⁰⁰ Id, paras. 24-27.

¹⁰¹ Human Rights Committee, General Comment No. 36 (2018) on article 6 of the International Covenant on Civil and Political Rights, on the right to life, para. 26.

¹⁰² Charles A. Reich, ‘Individual Rights and Social Welfare: The Emerging Legal Issues’, 74 *Yale L.J.* (1965), p. 1245.

¹⁰³ Michel Foucault, *Discipline and Punish: The Birth of the Prison* (1991), p. 222.

is unprecedented, which “has enabled it to elude systematic contest because it cannot be adequately grasped with our existing concepts.”¹⁰⁴ This private surveillance is being reinforced by trends in government surveillance. Jack Balkin has described the ‘National Surveillance State’ as “a permanent feature of governance [that] will become as ubiquitous in time as the familiar devices of the regulatory and welfare states.”¹⁰⁵

59. Digital technologies are employed in the welfare state to surveil, target, harass and punish beneficiaries, especially the poorest and most vulnerable among them. Once again, many of the submissions received by the Special Rapporteur serve to illustrate and reinforce this point. They serve to highlight a number of human rights concerns. First, in the context of social security benefits and assistance, there is a real risk that beneficiaries are effectively forced to give up their right to privacy and data protection to receive their right to social security as well as other social rights.¹⁰⁶

60. A second concern is the blurring of the lines between public and private surveillance. Welfare state authorities increasingly rely, either actively or passively, on private corporations for the surveillance and targeting of beneficiaries. Private entities have different motives for their involvement in benefit and social assistance systems and this may lead to conflicts between the public interests these systems ought to serve and the private interests of corporations and their owners.

61. A third concern is the potential for deliberate targeting and harassment of the poor through new technologies in the welfare state. As one submission to the Special Rapporteur highlights, fraud in the welfare state is often the result of confusion, complexity and the inability to correct the resulting errors.¹⁰⁷ But by deliberately using the power of new technologies to identify fraud or violations of ‘conditionalities’ imposed on beneficiaries, governments are likely to find inconsistencies that they can hold against claimants. It is relevant here that new technologies are enabling what Jack Balkin described as the ‘death of amnesia’: new abilities to collect information and store it digitally for an undefined period of time create a future in which a wealth of information can be held against someone indefinitely.¹⁰⁸

62. Additional concerns which warrant greater consideration than can be provided in the present report include (i) the human rights consequences of the move to predicting risk instead of the ex post enforcement of rules violations;¹⁰⁹ (ii) the dangers of connecting government data siloes which is more readily contemplated in the welfare context than elsewhere in the field of digital governance;¹¹⁰ (iii) the psychological and societal cost of constant monitoring and surveillance;¹¹¹ and (iv) the growing tendency of some governments to use the opportunities provided by the digital welfare state to try to alter social behaviours whether in the form of sexual activity or preferences, approaches to cohabitation, the use of alcohol or drugs, the decision to have children, or many other such goals.¹¹²

¹⁰⁴ Shoshana Zuboff, *The Age of Surveillance Capitalism* (2019), p. 14.

¹⁰⁵ Jack Balkin, ‘The Constitution in the National Surveillance State’, *Minnesota Law Review* (Vol. 93, 2008), p. 1-18.

¹⁰⁶ Submission to the Special Rapporteur by the Government of Mexico; Statement on Visit to the USA, by Professor Philip Alston, United Nations Special Rapporteur on extreme poverty and human rights, 15 December 2017, para 57.

¹⁰⁷ International Confederation of Trade Unions, at <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/ITCU.pdf>.

¹⁰⁸ Jack Balkin, ‘The Constitution in the National Surveillance State’, *Minnesota Law Review* (Vol. 93, 2008), p. 13.

¹⁰⁹ Id, p. 11.

¹¹⁰ https://www.washingtonpost.com/news/theworldpost/wp/2018/08/09/aadhaar/?utm_term=.8a17992dfb6e.

¹¹¹ “In our research with civil society groups ... concerns about stigmatisation and feelings of being targeted were more prominent than privacy concerns per se.” Data Justice Lab, at <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/UniversityCardiff.pdf>.

¹¹² Cf Foucault’s analysis of Panoptic systems that could “be used as a machine to carry out experiments, to alter behaviour, to train and correct individuals”. Michel Foucault, *Discipline and Punish: The Birth of the Prison* (1991), p. 203.

F. Resisting the inevitability of a digital only future

63. Digital technologies in general, and especially those central to the digital welfare state, are often presented as being both unavoidable and irresistible. If a country wants to be seen to be at the technological cutting edge, if its government wants to have the most efficient, economical and flexible welfare system available, and if its citizenry wants all of the convenience that comes from not having to provide ID in order to undertake various transactions, then a transition to a digital welfare state must be pursued. But quite apart from the choices that citizens and governments might make if they were fully informed and adequately consulted, the reality is that such decisions are all too often taken in the absence of sophisticated cost-benefit analyses. And when such analyses are undertaken, they consist of financial balance sheets that ignore what might be termed the fiscally invisible intangibles that underpin human rights. Values such as dignity, choice, self-respect, autonomy, self-determination, privacy, and a range of other factors are all traded off without being factored into the overall equation, all but guaranteeing that insufficient steps will be taken to ensure their role in the new digital systems.

64. It is often assumed that at least some of these tradeoffs can be justified on the grounds that the bargain is just a matter between the individual and a particular government agency. But such an image is increasingly very far from the truth as cross-matching, data sharing, and cross-verification systematically enlarge the pools of data potentially available across the spectrum of government. To the extent that assurances are given that leakage from one silo to the next will not occur, such guarantees are largely illusory since a change of government or a real or imagined emergency situation is all that is required to trigger a partial or comprehensive breaking down of the partitions, quite apart from the risks of electronic data breaches due to hacking or normal system breakdowns. In addition, the assumption that the relationship is only that between government and citizen is also anachronistic. Corporate actors are now centrally involved in large parts of the welfare system, and when taken together with the ever-expanding reach of other forms of surveillance capitalism, intangible human rights values can be assumed to be worth as much as the shares of a bankrupt corporation.

65. The Special Rapporteur has learned of situations in which crucial decisions to go digital have been taken by government ministers without consultation, or even by departmental officials without any significant policy discussions taking place, on the grounds that the move is essentially an administrative matter, rather than involving a potentially game-changing approach to a large swathe of official policy. Sometimes there seems to be a presumption that even if the move to digital is not currently necessary, it surely will be one day and it is better to move in advance. Support for such pre-emptive moves may come from corporate interests, as well as from the security and counter-terrorism sectors, albeit for quite different reasons. Careful and transparent consideration should always be given to the questions of why, for whom, when, and how transitions to digital systems take place.

66. And even where detailed cost estimates are provided, this is an area in which accuracy seems difficult to achieve. Helen Margetts has observed that in the United Kingdom, for example, “[t]echnology and the public sector have rarely been happy bedfellows” and “every government technology project seems doomed to arrive late, underperform and come in over budget.”¹¹³ Another example is the Aadhaar system in India which is said to have lacked a proper cost-benefit analysis prior to implementation¹¹⁴ and in relation to which there has been great disagreement as to the post hoc assessment of costs and benefits.¹¹⁵

¹¹³ <https://theconversation.com/back-to-the-bad-old-days-as-civil-service-infighting-threatens-uks-only-hope-for-digital-government-47683>.

¹¹⁴ National Law University Delhi, at <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/NationalLawUniversityDelhi.pdf>.

¹¹⁵ Reetika Khera, ‘A ‘Cost-benefit’ Analysis of UID’, *Economic and Political Weekly*, Vol. 48, No. 5 (2 February, 2013), p. 13-15; <https://www.iisd.org/gsi/subsidy-watch-blog/estimating-impact-indias-aadhaar-scheme-lpg-subsidy-expenditure>; <https://economictimes.indiatimes.com/blogs/et-commentary/aadhaars-11-bn-question/>; <https://thewire.in/economy/the-curious-case-of-the-world->

G. The role of the private sector

67. Two consistent themes of this report have been the reluctance of many governments to regulate the activities of technology companies, and the strong resistance of those companies to taking any systematic account of human rights considerations. The fact that this leads to many large technology corporations operating in an almost human rights free-zone is further exacerbated by the extent to which the private sector is taking a leading role in designing, constructing, and even operating significant parts of the digital welfare state.¹¹⁶

68. Among well-known examples are the involvement of Net 1 subsidiary Cash Paymaster Services (CPS), MasterCard and Grindrod Bank in the distribution of social grants linked to South Africa's biometric identification system, the roles played by Indue and Visa in the Cashless Debit Card trials in Australia, and IBM's involvement in Ontario's Social Assistance Management System. Submissions to the Special Rapporteur have also drawn attention to the increasing role of the private sector in the German market for public administration software used for unemployment services, social and youth welfare;¹¹⁷ and outsourcing by United Kingdom local authorities to private companies in the area of social protection.¹¹⁸ In contrast, various submissions point to the deliberate choice by governments involved *not* to rely on private actors to play key roles in the welfare state.¹¹⁹

69. The Special Rapporteur has addressed elsewhere the issues arising out of the privatization of public services more generally.¹²⁰ But in relation to social protection services there is a deeply problematic lack of information about the precise role and responsibility of private actors in proposing, developing and operating digital technologies in welfare states around the world. This lack of transparency has a range of causes, from gaps in freedom of information laws, confidentiality clauses, and intellectual property protections, through a failure on the part of legislatures and executives to require transparency, to a general lack of investigation of these practices by oversight bodies and the media.¹²¹ The absence of information seriously impedes efforts to hold governments and private actors accountable.

H. Accountability mechanisms

70. Many of the programs used to promote the digital welfare state have been designed by the very same companies that are so deeply resistant to abiding by human rights standards. Moreover those companies and their affiliates are increasingly relied upon to design and implement key parts of the actual welfare programs. It is thus evident that the starting point for efforts to ensure human rights-compatible digital welfare states outcomes is to ensure

bank-and-aadhaar-savings; and <https://qz.com/india/1519209/why-india-cant-cite-world-bank-to-brag-about-aadhaar/>.

¹¹⁶ Government of Ireland, at

<https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/Ireland.pdf>; Government of Estonia, at <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/Estonia.docx>; Submission to the Special Rapporteur by the Government of Croatia.

¹¹⁷ AlgorithmWatch, at

<https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/AlgorithmWatch.pdf>.

¹¹⁸ Data Justice Lab, at

<https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/UniversityCardiff.pdf>.

¹¹⁹ University of Auckland, at

<https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/UniversityAuckland.docx>; Submission to the Special Rapporteur by the Government of Greece; Submission to the Special Rapporteur by the Government of Argentina.

¹²⁰ A/73/396 (2018).

¹²¹ AlgorithmWatch, at

<https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/AlgorithmWatch.pdf>; Privacy International, at <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/PrivacyInternational.pdf>; Irish Council for Civil Liberties, at <https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/IrishCouncilCivilLiberties.pdf>.

through governmental regulation that technology companies are legally required to respect applicable international human rights standards.¹²²

IV. Conclusions

71. There is no shortage of analyses warning of the dangers for human rights of various manifestations of digital technology and especially artificial intelligence. But these studies focus overwhelmingly on the traditional civil and political rights such as the right to privacy, non-discrimination, fair trial rights, and the right to freedom of expression and information. With a handful of exceptions, none has adequately captured the full array of threats represented by the emergence of the digital welfare state. The vast majority of states spend very large amounts of money on different forms of social protection, or welfare, and the allure of digital systems that offer major cost savings along with personnel reductions, greater efficiency, and fraud reduction, not to mention the kudos associated with being at the technological cutting edge, is irresistible. There is little doubt that the future of welfare will be integrally linked to digitization and the application of AI.

72. But as humankind moves, perhaps inexorably, towards the digital welfare future it needs to alter course significantly and rapidly to avoid stumbling zombie-like into a digital welfare dystopia. Such a future would be one in which: unrestricted data matching is used to expose and punish the slightest irregularities in the record of welfare beneficiaries (while assiduously avoiding such measures in relation to the well-off); evermore refined surveillance options enable around the clock monitoring of beneficiaries; conditions are imposed on recipients that undermine individual autonomy and choice in relation to sexual and reproductive choices, and in relation to food, alcohol and drugs and much else; and highly punitive sanctions are able to be imposed on those who step out of line.

73. It will reasonably be objected that this report is unbalanced, or one-sided, because the dominant focus is on the risks rather than on the many advantages potentially flowing from the digital welfare state. The justification is simple. There are a great many cheerleaders extolling the benefits, but all too few counselling sober reflection on the downsides. Rather than seeking to summarize the analysis above, a number of additional observations are in order.

74. First, digital welfare state technologies are not the inevitable result of ‘scientific’ progress, but instead reflect political choices made by humans. Assuming that technology reflects pre-ordained or objectively rational and efficient outcomes risks abandoning human rights principles along with democratic decision-making.

75. Second, if the logic of the market is consistently permitted to prevail it inevitably disregards human rights considerations and imposes “externalities on society, for example when AI systems engage in bias and discrimination ... and increasingly reduce human autonomy”.¹²³

76. Third, the values underpinning and shaping the new technologies are unavoidably skewed by the fact that there is “a diversity crisis in the AI sector across gender and race”.¹²⁴ Those designing AI systems in general, as well as those focused on the welfare state are overwhelmingly white, male, well-off, and from the Global North.

¹²² See Yeung et al, above; Paul Nemitz, ‘Constitutional Democracy and Technology in the Age of Artificial Intelligence’, *Philosophical Transactions*, A 376 (2018); and Karen Yeung, ‘A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework’, Council of Europe doc. MSI-AUT(2018)05 rev (22 May 2019).

¹²³ Anton Korinek, ‘Integrating Ethical Values and Economic Value to Steer Progress in Artificial Intelligence’ (2019) p. 2, at <http://www.nber.org/papers/w26130>.

¹²⁴ Sarah West, Meredith Whittaker, and Kate Crawford, *Discriminating Systems: Gender, Race and Power in AI* (AI Now Institute, 2019) (Women make up “15% of AI research staff at Facebook and 10% at Google. ... [and] only 2.5% of Google’s workforce is black, while Facebook and Microsoft are each at 4%.”).

No matter how committed they might be to certain values, the assumptions and choices made in shaping the digital welfare state will reflect certain perspectives and life experiences. The way to counteract these biases and to ensure that human rights considerations are adequately taken into account is to ensure that the “practices underlying the creation, auditing, and maintenance of data” are subjected to very careful scrutiny.¹²⁵

77. Fourth, predictive analytics, algorithms and other forms of AI are highly likely to reproduce and exacerbate biases reflected in existing data and policies. In-built forms of discrimination can fatally undermine the right to social protection for key groups and individuals. There therefore needs to be a concerted effort to identify and counteract such biases in designing the digital welfare state. This in turn requires transparency, and broad-based inputs into policy-making processes. The public, and especially those directly affected by the welfare system, need to be able to understand and evaluate the policies that are buried deep within the algorithms.

78. Fifth, especially but not only in the Global North, the technology industry is heavily oriented towards designing and selling gadgets for the well-off such as driverless and flying cars and electronic personal assistants for multi-tasking businessmen [sic]. In the absence of fiscal incentives, government regulation, and political pressures, it will devote all too little attention to facilitating the creation of a welfare state that takes full account of the humanity and concerns of the less well-off in any society.

79. Sixth, to date astonishingly little attention has been paid to the ways in which new technologies might transform the welfare state for the better. Instead of obsessing about fraud, cost savings, sanctions, and market-driven definitions of efficiency, the starting point should be on how existing or even expanded welfare budgets could be transformed through technology to ensure a higher standard of living for the vulnerable and disadvantaged, to devise new ways of caring for those who have been left behind, and more effective techniques for addressing the needs of those who are struggling to enter or re-enter the labour market. That would be the real digital welfare state revolution.

¹²⁵ Rashida Richardson, Jason M. Schultz, and Kate Crawford, ‘Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice’, 94 *New York University Law Review* (2019) 192, at 225.